Přehled zpráv

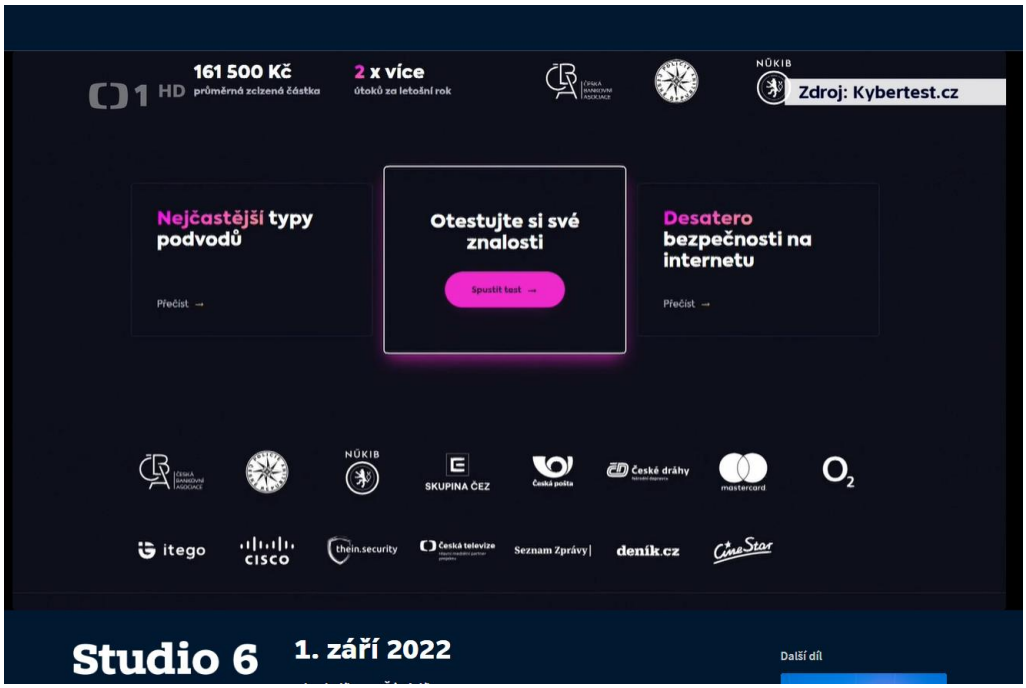
1. Studio 6: 1. září

Televize ● Studio 6 (ČT1) ● 1. 9. 2022, 5:59

Vydavatel: **ČESKÁ TELEVIZE (cz-00027383)**

Dosah: 79 759 ● GRP: 0.89 ● OTS: 0.01 ● AVE: 18839474.59 Kč

Odkaz: https://www.ceskatelevize.cz/porady/1096902795-studio-6/222411010100901/



2. Počet kyberútoků na klienty bank stoupl za dva roky čtyřnásobně

Online ● ceskenoviny.cz (Zprávy / Politika) ● 1. 9. 2022, 8:16

Vydavatel: **Česká tisková kancelář (cz-47115068)** ● Autor: **ČTK**

Dosah: 165 971 ● GRP: 1.84 ● OTS: 0.02 ● AVE: 34288.69 Kč

Odkaz: https://www.ceskenoviny.cz/zpravy/pocet-kyberutoku-na-klienty-bank-stoupl-za-dva-roky-ctyrnasobne/2250488

Počet kyberútoků na klienty bank stoupl za dva roky čtyřnásobně

Aktualizace: 01.09.2022 10:16 Vydáno: 01.09.2022, 10:16

Počítač, notebook, internet, nákup, platební karta, e-shop - ilustrační foto. ČTK/WAVEBREAK/Wavebreak Media LTD

Praha - Počet kybernetických útoků na klienty tuzemských bank se za poslední dva roky zvýšil čtyřnásobně. Škoda na jednoho poškozeného klienta dosáhla v průměru 161.500 Kč. Vyplývá to z údajů České bankovní asociace. Spolu s orgány státní správy a velkými firmami dnes spustila rozsáhlou vzdělávací kampaň #nePINdej!, která poběží

do prosince.

"Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší, než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším," uvedla výkonná ředitelka ČBA Monika Zahálková na tiskové konferenci.

Český finanční sektor patří podle Národního úřadu pro kybernatickou a informační bezpečnost (NÚKIB) k nejlépe zabezpečeným, přesto 81 procent finančních institucí zaznamenalo pokus o útok. Nejčastějšími typy útoků byly phishing, podvodné e-maily a škodlivé kódy. Narostlo rovněž množství podvodů na sociálních sítích a loňskou novinkou byly reverzní inzertní podvody, kdy podvodníci oslovují prodávající na internetových bazarech a snaží se od nich získat údaje k platebním kartám. Podle ředitele NÚKIB Lukáše Kintra nelze očekávat, že by se jejich míra měla snižovat.

Na rostoucí nebezpečí podvodů na internetu má upozornit rozsáhlá vzdělávací kampaň. Klíčovým prvkem kampaně je interaktivní vzdělávací Kybertest na stránkách www.kybertest.cz. Test zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. Kybertest má několik variant, které simulují nejčastější podvodné praktiky podle různých věkových skupin. "Jiné otázky se tedy generují pro teenagery a jiné pro seniory. Stejně tak jako útoky hackerů. Jiné praktiky zkoušejí na mladší generaci, jiné pak na starší a nejstarší spoluobčany," dodal člen představenstva společnosti itego, která test vytvořila, Tomáš Trachta.

Do kampaně jsou vedle České bankovní asociace zapojeni NÚKIB, Policie ČR, itego, Cisco, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy. Mediálními partnery jsou Česká televize, Seznam Zprávy, Deník a Cinestar.

KRIMINALITA BANKY INTERNET ČBA

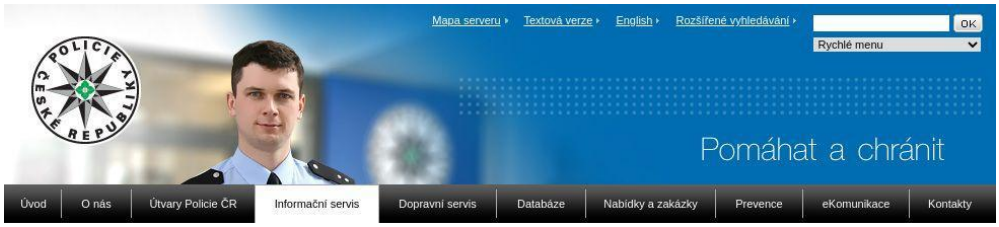
Autor: ČTK Líbí se 0 Vytisknout

3. #nePINdej!

Online ● policie.cz (Jiné) ● 1. 9. 2022, 10:00

Dosah: 20 667 ● GRP: 0.23 ● OTS: 0.00 ● AVE: 19996.45 Kč ● Interakcí: 4

Odkaz: https://www.policie.cz/clanek/nepindej.aspx



ZPRAVODAJSTVÍ

Úvodní strana / Informační servis / Zpravodajství

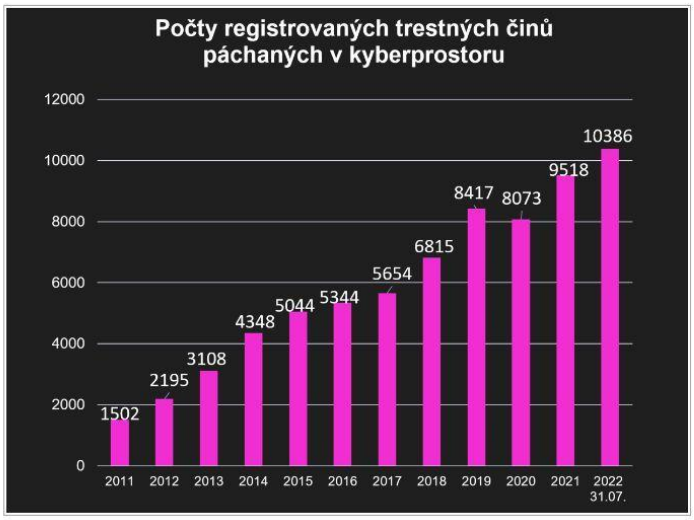
#nePINdej!

Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů. Police ČR se dnešním dnem připojuje k rozsáhlé vzdělávací kampani České bankovní asociace a dalších partnerů, která upozorňuje na sílící nebezpečí podvodů na internetu.

Jak vyplývá z dat České bankovní asociace získaných od jejích členských bank, na jednoho poškozeného klienta připadá průměrná škoda ve výši 161 500 korun. U vishingu, neboli případů podvodného navolávání, jsou částky až čtvrtmilionové.

Klíčovým prvkem kampaně s názvem **#nePINdej!** (kreativní tvorba ze slov PIN nedej) je interaktivní vzdělávací **www.kybertest.cz**, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. Kybernetická kriminalita již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Kampaň proto cílí na širokou veřejnost počínaje dětmi a mladistvými přes dospělé až na seniory. *„Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na nejstarší spoluobčany."* vysvětluje **Tomáš Trachta, člen představenstva společnosti itego, a.s.**, která pro ČBA kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně.

V kybertestu jsou simulovány podvodné SMS, zobrazovací okna k připojení k WIFI sítím, phishingové emaily, zvukové nahrávky podvodných telefonů a mnohé další, tak, aby si je každý uživatel moderních technologií mohl bezpečně vyzkoušet. Testové otázky byly připravovány odborníky na základě reálných případů, jimiž se podvodníci snaží své oběti nachytat. Kampaň #nePINdej! patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají. *„Zároveň bude na sociálních sítích i v dalších kanálech aktivizovat veřejnost k tomu, aby si ve speciálně vytvořené online aplikaci otestovala své schopnosti obstát před kyberútoky,"* říká **Monika Zahálková, výkonná ředitelka České bankovní asociace**.



Počty registrovaných TČ páchaných v kyberprostoru

Pachatelé se při těchto útocích snaží překonávat zejména lidský faktor a pod nejrůznějšími legendami využívají nátlaku, strachu a časové tísně pro záchranu peněz nebo pro realizaci finanční transakce. Mezi nejčastější podvodné legendy patří:

Podvodné navolávání:

- Pachatelé se vydávají například za bankéře, policisty, pracovníky technické podpory a snaží se z lidí pod vlivem strachu vylákat peníze, nebo vzdálený přístup do zařízení oběti, který následně zneužije.

Nabídka výhodných investic:

MVČR

Hasiči ČR

SOUVISEJÍCÍ ODKAZY

- Zpravodajství
- Zpravodajství - archiv
- Zpravodajství - kraje
- Odbor komunikace a vnějších vztahů

- Přesvědčivá lákavá reklama a manipulativní jednání. Cílem pachatele je vylákat z oběti co možná nejvíce finančních prostředků a využívá k tomu přirozenou ziskuchtivost každého z nás.

Reverzní inzertní podvody:

- Pachatel zareaguje na váš inzerát. Podstrčí vám fiktivní platební bránu, kde vyplníte citlivé bankovní údaje a místo peněz za inzerované zboží přicházíte o všechny úspory.

Podvody typu Nigerijské dopisy:

- Princip, který funguje už více jak 100 let. Pachatelé sázejí na kvantitu. Vždy se najde někdo, kdo se nechá nachytat na slibovanou cennou zásilku nebo domnělou pomoc. Často zde hraje velkou roli láska.

Klasické podvody typu phishing a smishing:

- Stále dokonalejší a složitě rozpoznatelné podvodné emaily a SMS nabídky. Na první pohled již nenajdeme podezřelé znaky.

Kromě tradičních podvodných e-mailů, SMS a již zmíněného vishingu se stále častěji setkáváme s podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze. *„Loňskou novinkou jsou také tzv. reverzní inzertní podvody, jejichž počet neustále roste. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovování údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou,"* objasnil **brig. gen. Tomáš Kubík, náměstek policejního prezidenta pro kriminální policii**.

Kyberkampaň #nePINdej! bude s ohledem na širokou cílovou skupinu probíhat napříč všemi médii – na internetu, v tisku, v České televizi, využita bude i tištěná reklama – formou letáků na pobočkách České pošty –, a pevné reklamní plochy ve vlacích a na nádražích Českých drah, ale i na bankomatech bank působících na českém trhu. Společnost O2 pak kampaň podpoří SMS zprávami s výzvou k účasti na testu. Ze sociálních sítí bude kromě standardních kanálů (Facebook, LinkedIn, Twitter, Instagram) nově využit i TikTok. Kampaň podpoří na svých profilech i influencer Martin „Mikýř" Mikyska.

Základní rady, jak nenaletět

- Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.
- Vyzkoušej si **www.kybertest.cz** a zjisti, kde máš mezery. Buď připraven.

plk. Zuzana Pidrmnaová
vedoucí oddělení prevence

Leták nePINdej

Detailní náhled

Související dokumenty

nePINdej TZ pro marketingová media final.docx
Velikost souboru:194,1 KB / formát DOCX

TZ Kybertest final.docx
Velikost souboru:194,3 KB / formát DOCX

Kyberkampaň - prezentace.pptx
Velikost souboru:11,4 MB / formát PPTX

E-mailem Vytisknout

4. Nesdílet bankovní údaje, hesla a nepodléhat nátlaku. Startuje kampaň nePINdej

Online ● ct24.ceskatelevize.cz (Zprávy / Politika) ● 1. 9. 2022, 10:47

Vydavatel: **ČESKÁ TELEVIZE (cz-00027383)** ● Autor: **ško** ● Rubrika: **Internet**

Dosah: 241 450 ● GRP: 2.68 ● OTS: 0.03 ● AVE: 46933.02 Kč ● Interakcí: 18

Odkaz: https://ct24.ceskatelevize.cz/domaci/3526307-nesdilet-bankovni-udaje-hesla-a-nepodlehat-natlaku-startuje-kampan-nepindej

Počet útoků se za poslední dva roky zvýšil až čtyřnásobně, i proto se spouští vzdělávací kampaň proti podvodníkům na internetu. Expert na bankovní a finanční bezpečnost České bankovní asociace Petr Barák ČT sdělil, že nejčastější chybou klientů je, že poskytnou cizím lidem přístupové údaje ke svým účtům do mobilního či internetového bankovnictví.

Častým útokem je takzvaný vishing, kdy někdo zavolá pod hlavičkou banky a snaží se vytvořit dojem, že peníze jsou v ohrožení, případně nabízí jejich lepší zhodnocení. Klienti této lži uvěří a začnou s pachateli spolupracovat. Ti je pak podle Baráka „dovedou, kam potřebují“ a nakonec si nechají vyzradit přístupové údaje k účtu, z nějž odčerpají peníze.

Zneužití strachu

Vedoucí oddělení prevence Policejního prezidia Zuzana Pidrmanová doplnila, že klienti jsou často velmi důvěřiví. Bojí se o peníze, což podle ní může ještě zvyšovat tlak sdělovacích prostředků, které informují o inflaci a zdražování. Podvodníkům tak nahrává strach, kvůli němuž jsou více náchylní k manipulacím a nátlaku. Pachatelé totiž často operují i s údajným časovým limitem, kdy se celá akce musí odehrát.

Pidrmanová vysvětlila, že útočníci pracují tak, aby nezanechali stopy, používají například jednorázové datové linky či mobilní telefony. Nechce však vyvolávat paniku, policie si podle ní umí s těmito případy poradit – to však neznamená, že lze všechno zachránit. I kvůli rychlosti pachatelů, kdy se celý podvod děje v řádu minut a samotné převody jsou vteřinové.

Edukovat klienty bank a ukázat jim rizika má kampaň na stránkách kybertest.cz. Lidé si tam mohou udělat kvíz, v němž mají rozpoznat podvodné stránky, praktiky či telefonáty a bezpečně se pohybovat na internetu.

Jak se bránit?

Základem je zabezpečení telefonu či počítače, silná hesla a PIN kódy, je také nutné používat pouze pravé a certifikované aplikace bank nebo prověřené e-shopy. Je důležité nikomu nesdělovat přihlašovací údaje. Banka přihlašovací údaje nikdy nežádá, a už vůbec ne telefonicky, e-mailem anebo prostřednictvím sociálních sítí.

Odborníci apelují neotvírat e-maily ani přílohy od neznámých a podezřelých odesílatelů a neklikat ani na žádné odkazy v těle těchto e-mailů. Vždy je třeba zkontrolovat e-mailovou adresu odesílatele a pravopis.

Pokud má člověk byť jen podezření, že se s účtem děje něco podivného či špatného, má kontaktovat svou banku. Přes infolinku zákaznická podpora dokáže zkontrolovat účet, zablokovat příkazy nebo ztracenou kartu.

5. Počet kyberútoků na klienty bank stoupl za dva roky čtyřnásobně

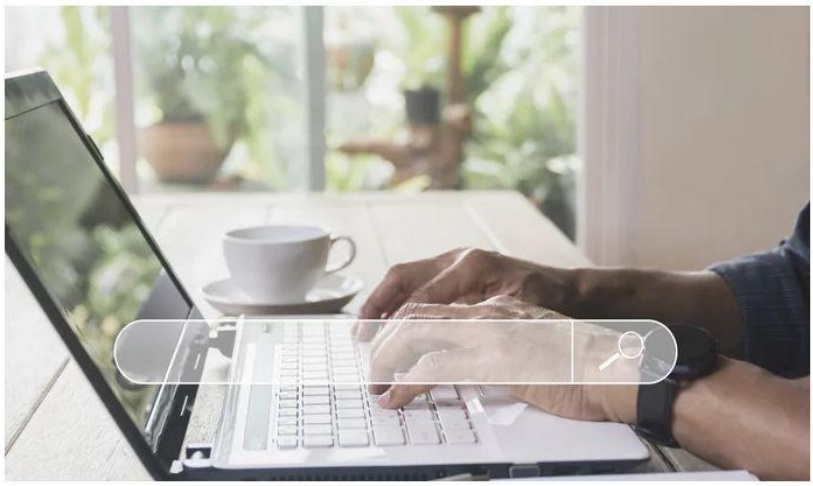
Online ● e15.cz/finexpert (Ekonomika / Finance / Právo) ● 1. 9. 2022, 11:10

Vydavatel: **CZECH NEWS CENTER a.s. (cz-02346826)** ● Autor: **ČTK**

Dosah: 76 245 ● GRP: 0.85 ● OTS: 0.01 ● AVE: 20000.00 Kč

Odkaz: https://www.e15.cz/finexpert/setrime/pocet-kyberutoku-na-klienty-bank-stoupl-za-dva-roky-ctyrnasobne-1392778

Počet kyberútoků na klienty bank stoupl za dva roky čtyřnásobně



ilustrační foto • *ZDROJ: ProfiMedia*

ČTK
1. září 2022 • 11:10

"Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší, než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším," uvedla výkonná ředitelka ČBA Monika Zahálková na tiskové konferenci.

Český finanční sektor patří podle Národního úřadu pro kybernatickou a informační bezpečnost (NÚKIB) k nejlépe zabezpečeným, přesto 81 procent finančních institucí zaznamenalo pokus o útok. Nejčastějšími typy útoků byly phishing, podvodné e-maily a škodlivé kódy. Narostlo rovněž množství podvodů na sociálních sítích a loňskou novinkou byly reverzní inzertní podvody, kdy podvodníci oslovují prodávající na internetových bazarech a snaží se od nich získat údaje k platebním kartám. Podle ředitele NÚKIB Lukáše Kintra nelze očekávat, že by se jejich míra měla snižovat.

Nakupujeme

Hackeři útočí prostřednictvím podvodných telefonátů, cílí na klienty bank

Na rostoucí nebezpečí podvodů na internetu má upozornit rozsáhlá vzdělávací kampaň. Klíčovým prvkem kampaně je interaktivní vzdělávací Kybertest na stránkách www.kybertest.cz. Test zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. Kybertest má několik variant, které simulují nejčastější podvodné praktiky podle různých věkových skupin. "Jiné otázky se tedy generují pro teenagery a jiné pro seniory. Stejně tak jako útoky hackerů. Jiné praktiky zkoušejí na mladší generaci, jiné pak na starší a nejstarší spoluobčany," dodal člen představenstva společnosti itego, která test vytvořila, Tomáš Trachta.

Do kampaně jsou vedle České bankovní asociace zapojeni NÚKIB, Policie ČR, itego, Cisco, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy. Mediálními partnery jsou Česká televize, Seznam Zprávy, Deník a Cinestar.

Autor: ČTK

Klíčová slova: České dráhy Národní úřad pro kybernetickou a informační bezpečnost Česká televize ČEZ MasterCard Česká pošta podvod Cisco Systems Cinestar Česká bankovní asociace

6. Průměrná škoda u lidí okradených přes internet činí už přes 161 tisíc korun

Online ● pcworld.cz (IT / Technologie) ● 1. 9. 2022, 11:19

Vydavatel: **Internet Info DG, a.s. (cz-00565211)**

Dosah: 2 396 ● GRP: 0.03 ● OTS: 0.00 ● AVE: 12433.47 Kč

Odkaz: https://www.pcworld.cz/clanky/prumerna-skoda-u-lidi-okradenych-pres-internet-cini-uz-pres-161-tisic-korun/

„Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší, než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším," uvedla výkonná ředitelka ČBA Monika Zahálková.

Zveřejněné údaje potvrzují trend, o kterém nedávno mluvila i Policie České republiky. Z její statistiky vyplývá, že zatímco loni se pohybovala internetová kriminalita kolem šesti procent celkových nahlášených trestných činů, za první pololetí letošního roku je to už téměř deset procent.

Mezi nejčastější typy útoků patří phishing, podvodné e-maily nebo takzvané reverzní inzertní podvody, kdy podvodníci oslovují prodávající na internetových bazarech a snaží se od nich získat údaje k platebním kartám.

Česká bankovní asociace společně s dalšími soukromými subjekty, policií a Národním úřadě pro kybernetickou a informační bezpečnost spustila rozsáhlou vzdělávací kampaň. Jejím klíčovým prvkem je interaktivní vzdělávací Kybertest na stránkách www.kybertest.cz, který má veřejnost seznámit s nejčastějšími kybernetickými podvody a naučit ji, jak je rozpoznat a jak jim nenaletět.

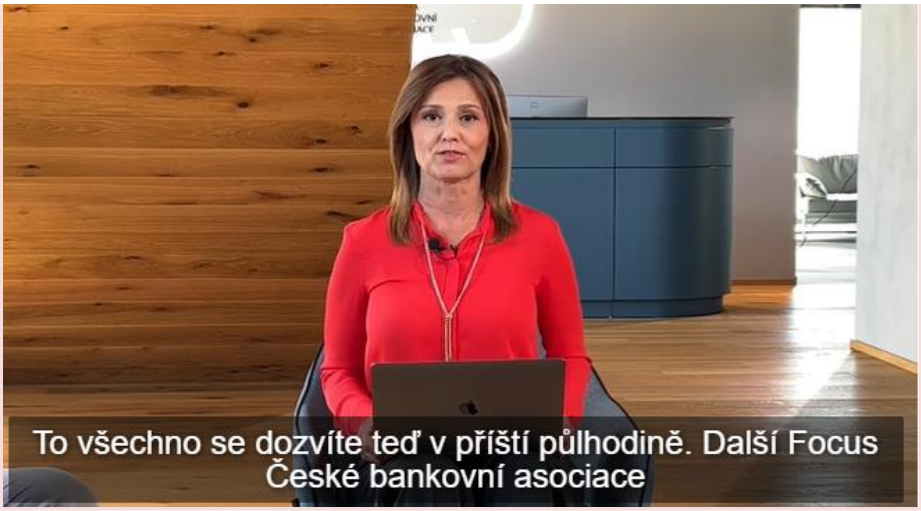
7. Každý druhý podvodný telefonát je úspěšný. Odborníci radí, jak si dát pozor

Online ● seznamzpravy.cz (Zprávy / Politika) ● 1. 9. 2022, 11:20

Vydavatel: **Seznam.cz, a.s. (cz-26168685)** ● Autor: **Petra Krmelová**

Dosah: 1 702 492 ● GRP: 18.92 ● OTS: 0.19 ● AVE: 79177.75 Kč ● Interakcí: 49

Odkaz: https://www.seznamzpravy.cz/clanek/ekonomika-byznys-rozhovory-kazdy-druhy-podvodny-telefonat-je-uspesny-odbornici-radi-jak-si-dat-pozor-212912



Focus České bankovní asociace cílí na problematiku kyberútoků. Sledujte jej živě ve čtvrtek 1. září od 11:30.

(Video: Seznam Zprávy)

11:20

● ŽIVĚ

Česká bankovní asociace ve spolupráci s orgány státní správy a klíčovými firmami českého byznysu spouští rozsáhlou celonárodní vzdělávací kampaň #nePINdej! Proti kyberútokům, kterých dramaticky přibývá a jsou stále rafinovanější.

Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů a na jednoho poškozeného klienta je to v průměru 161 500 korun. Vyplynulo to z dat České bankovní asociace (ČBA), získaných od jejích členských bank. O problematice kyberútoků a jak se jim bránit uspořádala asociace diskusi, kterou Seznam Zprávy jako mediální partner přenáší živě ve čtvrtek od 11:30.

Pozor na fotky, hovory a hesla. Česko se připravuje na kyberútoky

25. 4. 2021 13:34

„Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tak zvaný vishing, který patří k těm nejzákeřnějším. Zatímco před dvěma lety se jejich počet pohyboval v nízkých stovkách, letos mluvíme o desítkách tisíc," uvedla Monika Zahálková, výkonná ředitelka České bankovní asociace.

Hosté Focusu ČBA

TOMÁŠ KUBÍK, NÁMĚSTEK POLICEJNÍHO PREZIDENTA

JAN PINTA, EXPERT NA KYBERNETICKOU BEZPEČNOST, THEIN SECURITY

PETR BARÁK, EXPERT NA FINANČNÍ BEZPEČNOST ČBA

Focus ČBA živě přenášíme ve čtvrtek 1. září od 11:30.

A narostla i jejich úspěšnost. Téměř každý druhý podvodný telefonát v současné době končí škodou pro klienta. Průměrné částka, o kterou klienti při těchto útocích přijdou, je přitom dost vysoká, zhruba čtvrt milionu korun.

Její slova potvrzuje i Lukáš Kintr, ředitel Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

„Žijeme v digitální době, která nám mnohé věci usnadňuje, ale také přináší mnohá rizika, a mezi ně patří i rostoucí počet různých kyberútoků. Detekujeme vysoké počty nejen podvodných telefonátů, ale i textových zpráv či e-mailů, a nelze očekávat, že by se jejich míra měla snižovat."

Nejlepší obranou proti těmto pokusům podle něj nadále zůstává informovanost a poučenost veřejnosti, aby byli lidé schopni vishing a podobné snahy rozpoznat.

veřejnosti, aby byli lidé schopni vishing a podobné snahy rozpoznat.

Přibývá také způsobů, jimiž se podvodníci snaží své oběti nachytat. Kromě tradičních podvodných e-mailů, SMS a zmíněného vishingu se stále častěji objevují podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze.

Loňskou novinkou jsou také tak zvané reverzní inzertní podvody, jejichž počet neustále roste. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu „bezpečnou platbu“, tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru.

„Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou,“ vysvětluje Tomáš Kubík, náměstek policejního prezidenta pro kriminální policii.

#nePINdej! – celonárodní vzdělávací kampaň v oblasti kyberbezpečnosti

Kybernetická kriminalita také dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání.

Kampaň #nePINdej!

Patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti u nás. Zapojily se jak orgány státní správy, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají.

Kromě ČBA i Policie České republiky, Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), itego, a.s., CISCO, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy.

Mediálními partnery jsou Česká televize (hlavní mediální partner), Seznam Zprávy, Deník a Cinestar.

Česká bankovní asociace proto spouští rozsáhlou vzdělávací kampaň, která má upozornit na sílící nebezpečí podvodů na internetu. Pod názvem #nePINdej! představí nejčastější kybernetické útoky a formou hravého testu na www.kybertest.cz naučí, jak jim nenaletět. Kampaní chce ČBA oslovit širokou veřejnost. Mladistvé od 12 let, dospělé i seniory.

SDÍLEJTE ČLÁNEK

8. ČBA: Počet kyberútoků na klienty bank stoupl za dva roky čtyřnásobně

Online ● zlato.cz (Zprávy / Politika) ● 1. 9. 2022, 12:00

Vydavatel: **Zlato a.s. (cz-04403231)** ● Autor: **Denis Drahoš**

Dosah: 1 506 ● GRP: 0.02 ● OTS: 0.00 ● AVE: 6644.98 Kč

Odkaz: https://www.zlato.cz/magazin/cba-pocet-kyberutoku-na-klienty-bank-stoupl-za-dva-roky-ctyrnasobne/

ZLATO.CZ

Jistota ve vlastních rukou

PROJEKT ZLATO.CZ | KDO JSME | ANTI ROBIN HOOD | FAKTA | VIDEA A ROZHOVORY | D K Z

MAGAZÍN

ČBA: Počet kyberútoků na klienty bank stoupl za dva roky čtyřnásobně

Počet kybernetických útoků na klienty tuzemských bank se za poslední dva roky zvýšil čtyřnásobně. Škoda na jednoho poškozeného klienta dosáhla v průměru 161 500 Kč. Vyplývá to z údajů České bankovní asociace. Spolu s orgány státní správy a velkými firmami dnes spustila rozsáhlou vzdělávací kampaň #nePINdej!, která poběží do prosince.

Nejčastějšími typy útoků byly phishing, podvodné e-maily a škodlivé kódy. Narostlo rovněž množství podvodů na sociálních sítích a loňskou novinkou byly reverzní inzertní podvody, kdy podvodníci oslovují prodávající na internetových bazarech a snaží se od nich získat údaje k platebním kartám. Foto: iStock

„Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší, než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším," uvedla výkonná ředitelka ČBA Monika Zahálková na tiskové konferenci.

Český finanční sektor patří podle Národního úřadu pro kybernatickou a informační bezpečnost (NÚKIB) k nejlépe zabezpečeným, přesto 81 procent finančních institucí zaznamenalo pokus o útok. Nejčastějšími typy útoků byly phishing, podvodné e-maily a škodlivé kódy. Narostlo rovněž množství podvodů na sociálních sítích a loňskou novinkou byly reverzní inzertní podvody, kdy podvodníci oslovují prodávající na internetových bazarech a snaží se od nich získat údaje k platebním kartám. Podle ředitele NÚKIB Lukáše Kintra nelze očekávat, že by se jejich míra měla snižovat.

Na rostoucí nebezpečí podvodů na internetu má upozornit rozsáhlá vzdělávací kampaň. Klíčovým prvkem kampaně je interaktivní vzdělávací Kybertest na stránkách www.kybertest.cz. Test zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. Kybertest má několik variant, které simulují nejčastější podvodné praktiky podle různých věkových skupin. „Jiné otázky se tedy generují pro teenagery a jiné pro seniory. Stejně tak jako útoky hackerů. Jiné praktiky zkoušejí na mladší generaci, jiné pak na starší a nejstarší spoluobčany," dodal člen představenstva společnosti itego, která test vytvořila, Tomáš Trachta.

Do kampaně jsou vedle České bankovní asociace zapojeni NÚKIB, Policie ČR, itego, Cisco, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy. Mediálními partnery jsou Česká televize, Seznam Zprávy, Deník a Cinestar.

(ČTK)

1.9.2022, 12:00

9. ČBA: Počet kyberútoků na klienty bank stoupl za dva roky čtyřnásobně

Agenturní zpravodajství ● ČTK - Ekonomika (ČTK) ● 1. 9. 2022, 13:05

Vydavatel: **Česká tisková kancelář (cz-47115068)** ● Autor: **rot, jsa**

Odkaz: náhled

Praha 1. září (ČTK) - Počet kybernetických útoků na klienty tuzemských bank se za poslední dva roky zvýšil čtyřnásobně. Škoda na jednoho poškozeného klienta dosáhla v průměru 161.500 Kč. Vyplývá to z údajů České bankovní asociace. Spolu s orgány státní správy a velkými firmami dnes spustila rozsáhlou vzdělávací kampaň #nePINdej!, která poběží do prosince.
"Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším," uvedla výkonná ředitelka ČBA Monika Zahálková na tiskové konferenci.
Podle policejní statistiky přesáhl počet trestných činů páchaných v kyberprostoru od ledna do konce července jejich celkový počet z loňského roku. Zatímco letos policie eviduje již téměř 10.400 činů, loni to bylo za 12 měsíců zhruba 9500.
Český finanční sektor patří podle Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) k nejlépe zabezpečeným, přesto 81 procent finančních institucí zaznamenalo pokus o útok. Nejčastějšími typy útoků byly phishing, podvodné e-maily a škodlivé kódy. Narostlo rovněž množství podvodů na sociálních sítích a loňskou novinkou byly reverzní inzertní podvody, kdy podvodníci oslovují prodávající na internetových bazarech a snaží se od nich získat údaje k platebním kartám.
Podle ředitele NÚKIB Lukáše Kintra nelze očekávat, že by se jejich míra měla snižovat.
"Všichni si musíme uvědomit, že internet je čím dál nebezpečnější místo. Zlepšují se technické prostředky zabezpečení, mění se legislativa, ale to klíčové je kybernetické vzdělávání, prevence a také odpovědnost každého z nás za to, jaká data komu svěřujeme a s kým je sdílíme," uvedl výkonný ředitel platformy Kybez Michal Řezáč.
Na rostoucí nebezpečí podvodů na internetu má upozornit rozsáhlá vzdělávací kampaň. Klíčovým prvkem kampaně je interaktivní vzdělávací **Kybertest** na stránkách www.**kybertest**.cz. Test zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. **Kybertest** má několik variant, které simulují nejčastější podvodné praktiky podle různých věkových skupin. "Jiné otázky se tedy generují pro teenagery a jiné pro seniory. Stejně tak jako útoky hackerů. Jiné praktiky zkoušejí na mladší generaci, jiné pak na starší a nejstarší spoluobčany," dodal člen představenstva společnosti itego, která test vytvořila, Tomáš Trachta.
Do kampaně jsou vedle České bankovní asociace zapojeni NÚKIB, Policie ČR, itego, Cisco, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy. Mediálními partnery jsou Česká televize, Seznam Zprávy, Deník a Cinestar.
jsa rot
Autor: rot, jsa

10. Kybernetických útoků dramaticky přibývá a jsou stále rafinovanější

Online ● newsgate.cz (Zprávy / Politika) ● 1. 9. 2022, 13:27

Vydavatel: **Newsgate s.r.o. (cz-10977350)**

Dosah: 720 ● GRP: 0.01 ● OTS: 0.00 ● AVE: 4511.25 Kč

Odkaz: http://newsgate.cz/nejctenejsi/kybernetickych-utoku-dramaticky-pribyva-a-jsou-stale-rafinovanejsi/

#nePINdej!, která poběží do prosince.

> ***„Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším,“*** uvedla výkonná ředitelka ČBA Monika Zahálková na tiskové konferenci.

Podle policejní statistiky přesáhl počet trestných činů páchaných v kyberprostoru od ledna do konce července jejich celkový počet z loňského roku. Zatímco letos policie eviduje již téměř 10 400 činů, loni to bylo za 12 měsíců zhruba 9500.

Český finanční sektor patří podle Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) k nejlépe zabezpečeným, přesto 81 procent finančních institucí zaznamenalo pokus o útok. Nejčastějšími typy útoků byly phishing, podvodné e-maily a škodlivé kódy. Narostlo rovněž množství podvodů na sociálních sítích a loňskou novinkou byly reverzní inzertní podvody, kdy podvodníci oslovují prodávající na internetových bazarech a snaží se od nich získat údaje k platebním kartám. Podle ředitele NÚKIB Lukáše Kintra nelze očekávat, že by se jejich míra měla snižovat.

> ***„Všichni si musíme uvědomit, že internet je čím dál nebezpečnější místo. Zlepšují se technické prostředky zabezpečení, mění se legislativa, ale to klíčové je kybernetické vzdělávání, prevence a také odpovědnost každého z nás za to, jaká data komu svěřujeme a s kým je sdílíme,“*** uvedl výkonný ředitel platformy Kybez Michal Řezáč.

Na rostoucí nebezpečí podvodů na internetu má upozornit rozsáhlá vzdělávací kampaň. Klíčovým prvkem kampaně je interaktivní vzdělávací Kybertest na stránkách www.kybertest.cz. Test zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. Kybertest má několik variant, které simulují nejčastější podvodné praktiky podle různých věkových skupin.

> ***„Jiné otázky se tedy generují pro teenagery a jiné pro seniory. Stejně tak jako útoky hackerů. Jiné praktiky zkoušejí na mladší generaci, jiné pak na starší a nejstarší spoluobčany,“*** dodal člen představenstva společnosti itego, která test vytvořila, Tomáš Trachta.

Do kampaně jsou vedle České bankovní asociace zapojeni NÚKIB, Policie ČR, itego, Cisco, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy. Mediálními partnery jsou Česká televize, Seznam Zprávy, Deník a Cinestar.

11. Hackeři útočí na klienty českých bank čtyřikrát častěji

Online ● novinky.cz (Zprávy / Politika) ● 1. 9. 2022, 13:56

Vydavatel: **BORGIS a.s. (cz-00564893)**

Dosah: 1 991 104 ● GRP: 22.12 ● OTS: 0.22 ● AVE: 45000.00 Kč ● Interakcí: 4

Odkaz: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-hackeri-utoci-na-klienty-ceskych-bank-ctyrikrat-casteji-40407484

„Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším," uvedla výkonná ředitelka ČBA Monika Zahálková na tiskové konferenci.

Podle policejní statistiky přesáhl počet trestných činů páchaných v kyberprostoru od ledna do konce července jejich celkový počet z loňského roku. Zatímco letos policie eviduje již téměř 10 400 činů, loni to bylo za 12 měsíců zhruba 9500.

Vydávají se za exekutory, důvěřivce připraví o peníze
Bezpečnost

Phishing i podvodné e-maily

Český finanční sektor patří podle Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) k nejlépe zabezpečeným, přesto 81 procent finančních institucí zaznamenalo pokus o útok. Nejčastějšími typy útoků byly phishing, podvodné e-maily a škodlivé kódy. Narostlo rovněž množství podvodů na sociálních sítích a loňskou novinkou byly reverzní inzertní podvody, kdy podvodníci oslovují prodávající na internetových bazarech a snaží se od nich získat údaje k platebním kartám. Podle ředitele NÚKIB Lukáše Kintra nelze očekávat, že by se jejich míra měla snižovat.

„Všichni si musíme uvědomit, že internet je čím dál nebezpečnější místo. Zlepšují se technické prostředky zabezpečení, mění se legislativa, ale to klíčové je kybernetické vzdělávání, prevence a také odpovědnost každého z nás za to, jaká data komu svěřujeme a s kým je sdílíme," uvedl výkonný ředitel platformy Kybez Michal Řezáč.

Na rostoucí nebezpečí podvodů na internetu má upozornit rozsáhlá vzdělávací kampaň. Klíčovým prvkem kampaně je interaktivní vzdělávací Kybertest na stránkách www.kybertest.cz. Test zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. Kybertest má několik variant, které simulují nejčastější podvodné praktiky podle různých věkových skupin. „Jiné otázky se tedy generují pro teenagery a jiné pro seniory. Stejně tak jako útoky hackerů. Jiné praktiky zkoušejí na mladší generaci, jiné pak na starší a nejstarší spoluobčany," dodal člen představenstva společnosti itego, která test vytvořila, Tomáš Trachta.

Desatero bezpečného internetu

1. Důležité jsou pravidelné aktualizace celého počítače. Ty je nutné stahovat pro operační systém, bezpečnostní bránu (firewall), antivirus i další programy.

2. Některé viry dokážou bezpečnostní software v PC zablokovat. Proto je vhodné pravidelně kontrolovat, zdali funguje.

3. Škodlivé programy se často šíří prostřednictvím nevyžádané pošty. Pokud nevíte, od koho e-mail je, nikdy nestahujte jeho přílohu a neklikejte na žádné odkazy.

4. Pozor je nutné dávat na e-maily, v nichž odesílatel požaduje, abyste se přihlásili na nějakou webovou stránku a aktualizovali informace o vašem účtu.

5. Při zadávání přístupových hesel na internetových stránkách je nutné kontrolovat, zda je web zabezpečený. To poznáte například podle ikonky zámečku na liště internetového prohlížeče, nebo tak, že adresa webové stránky začíná zkratkou https, kde „s" znamená bezpečná.

6. Citlivé osobní informace zadávejte vždy pouze na internetových stránkách, které bezpečně znáte.

7. Do e-mailů nepatří důvěrné informace, jako je například číslo kreditní karty nebo heslo k bankovnímu účtu. Elektronickou poštu totiž může zachytit útočník.

8. Firewall dovoluje lépe zabezpečit operační systém. Méně zkušení uživatelé by jej rozhodně neměli vypínat. Při nedostatečných znalostech je vhodné jej nechat pracovat v automatickém režimu.

9. V internetových kavárnách a na cizích počítačích se nepřihlašujte do internetového bankovnictví. V počítači mohou být nainstalované keyloggery.

10. Obezřetnost je nutná při připojení k nezašifrovaným bezdrátovým sítím. Ty totiž může kdokoliv odposlouchávat a získat tak přístup ke všem datům v cizím počítači.

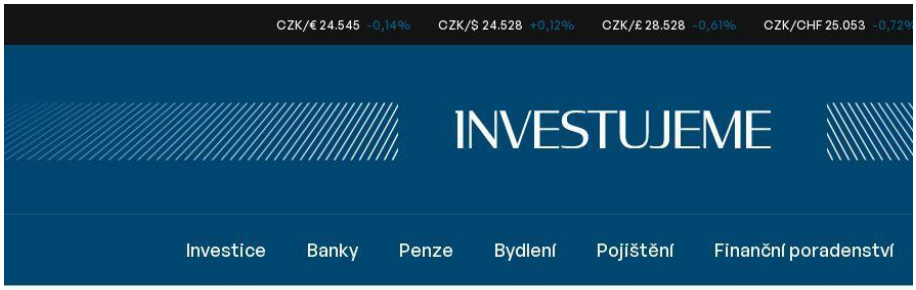
12. Kybernetických útoků dramaticky přibývá a jsou stále rafinovanější. ČBA proto spouští celonárodní vzdělávací kampaň #nePINdej!

Online ● investujeme.cz (Ekonomika / Finance / Právo) ● 1. 9. 2022, 14:10

Vydavatel: **Fincentrum & Swiss Life Select a.s. (cz-24260444)**

Dosah: 3 096 ● GRP: 0.03 ● OTS: 0.00 ● AVE: 9355.89 Kč

Odkaz: https://www.investujeme.cz/kratke-zpravy/kybernetickych-utoku-dramaticky-pribyva-a-jsou-stale-rafinovanejsi-cba-proto-spousti-celonarodni-vzdelavaci-kampan-nepindej/



01. 09. 2022

0 komentářů

Kybernetických útoků dramaticky přibývá a jsou stále rafinovanější. ČBA proto spouští celonárodní vzdělávací kampaň #nePINdej!

BANKY

Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů a na jednoho poškozeného klienta je to v průměru 161 500 korun. Vyplynulo to z dat České bankovní asociace (ČBA), získaných od jejích členských bank. ČBA proto ve spolupráci s orgány státní správy a s klíčovými firmami českého byznysu spouští rozsáhlou celonárodní vzdělávací kampaň #nePINdej!

„Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším. *Zatímco před dvěma lety se jejich počet pohyboval v nízkých stovkách, letos mluvíme již o desítkách tisíc. A narostla i jejich úspěšnost. Téměř každý druhý podvodný telefonát v současné době bohužel končí škodou pro klienta. Průměrné částka, o kterou klienti při těchto útocích přijdou, je přitom dost vysoká, zhruba čtvrt milionu korun,"* uvedla **Monika Zahálková, výkonná ředitelka České bankovní asociace**. Její slova potvrzuje i **Lukáš Kintr, ředitel Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB)**. *„Žijeme v digitální době, která nám mnohé věci usnadňuje, ale také přináší mnohá rizika, a mezi ně patří i rostoucí počet různých kyberútoků. Detekujeme vysoké počty nejen podvodných telefonátů, ale i textových zpráv či e-mailů, a nelze očekávat, že by se jejich míra měla snižovat. Nejlepší obranou proti těmto pokusům nadále zůstává obecná osvěta, tedy informovanost a poučenost veřejnosti, aby byli lidé schopni vishing a podobné snahy rozpoznat,"* upřesňuje **Lukáš Kintr**.

Přibývá také způsobů, jimiž se podvodníci snaží své oběti nachytat. Kromě tradičních podvodných e-mailů, SMS a již zmíněného vishingu se stále častěji setkáváme s podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze. *„Loňskou novinkou jsou také tzv. reverzní inzertní podvody, jejichž*

počet neustále roste. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou," objasnil **brig. gen. Tomáš Kubík, náměstek policejního prezidenta pro kriminální policii**.

#nePINdej! – celonárodní vzdělávací kampaň v oblasti kyberbezpečnosti

Kybernetická kriminalita také již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Česká bankovní asociace proto spouští rozsáhlou vzdělávací kampaň, která má upozornit na sílící nebezpečí podvodů na internetu. Pod názvem #nePINdej! představí nejčastější kybernetické útoky a formou hravého testu na www.kybertest.cz naučí, jak jim nenaletět. Kampaní chce ČBA oslovit širokou veřejnost – mladistvé od 12 let, dospělé i seniory.

Klíčovým prvkem kampaně #nePINdej! je interaktivní vzdělávací Kybertest, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. *„Název #nePINdej! funguje jako slovní hříčka a je vtipnou výzvou, aby si lidé dávali pozor na své citlivé údaje a chránili své peníze ve světě internetu. Zároveň bude na sociálních sítích i v dalších kanálech aktivizovat veřejnost k tomu, aby si ve speciálně vytvořené online aplikaci otestovala své schopnosti obstát před kyberútoky,"* říká **Monika Zahálková, výkonná ředitelka České bankovní asociace**.

Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. *„Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na nejstarší spoluobčany,"* vysvětluje **Tomáš Trachta, člen představenstva společnosti itego, a.s.**, která pro ČBA Kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně. Po spuštění testu dostane každý jeho účastník virtuální peníze do „hry", které musí před podvodnými útoky co nejlépe ochránit. Po každé otázce se lidé dozvědí správné řešení, mohou se z něj tak poučit a dalšímu simulovanému útoku následně nenaletět. *„Naším cílem není lidi nachytat a ukázat jim, jak špatně se v kyberprostoru pohybují. Naším cílem je především vzdělat a naučit co nejvíce občanů, jak praktiky podvodníků odhalit a jak se nenechat hackery okrást,"* vysvětluje **Monika Zahálková**.

Kampaň #nePINdej! zcela jistě patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají. Kromě České bankovní asociace, která je realizátorem projektu, jsou do kampaně zapojeny Policie České republiky, Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), itego, a.s., CISCO, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy. Mediálními partnery jsou Česká televize (hlavní mediální partner), Seznam Zprávy, Deník a Cinestar.

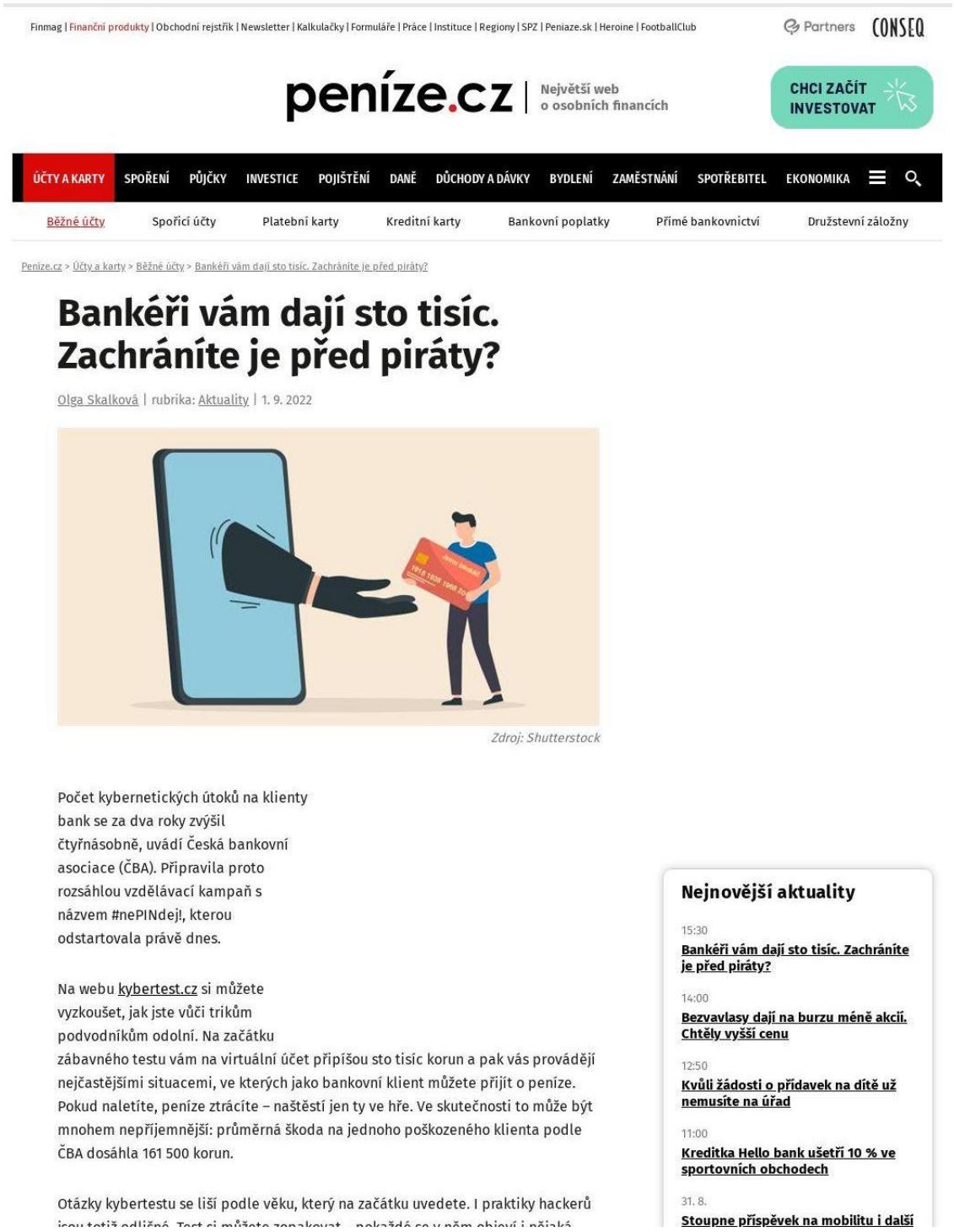
13. Bankéři vám dají sto tisíc. Zachráníte je před piráty?

Online ● penize.cz (Ekonomika / Finance / Právo) ● 1. 9. 2022, 15:30

Vydavatel: **NextPage Media, s.r.o. (cz-24780553)** ● Autor: **Olga Skalková**

Dosah: 160 492 ● GRP: 1.78 ● OTS: 0.02 ● AVE: 37842.83 Kč

Odkaz: https://www.penize.cz/bezne-ucty/436402-bankeri-vam-daji-sto-tisic-zachranite-je-pred-piraty



Finmag | Finanční produkty | Obchodní rejstřík | Newsletter | Kalkulačky | Formuláře | Práce | Instituce | Regiony | SPZ | Peniaze.sk | Heroine | FootballClub

Partners CONSEQ

peníze.cz | Největší web o osobních financích

CHCI ZAČÍT INVESTOVAT

ÚČTY A KARTY | SPOŘENÍ | PŮJČKY | INVESTICE | POJIŠTĚNÍ | DANĚ | DŮCHODY A DÁVKY | BYDLENÍ | ZAMĚSTNÁNÍ | SPOTŘEBITEL | EKONOMIKA

Běžné účty | Spořicí účty | Platební karty | Kreditní karty | Bankovní poplatky | Přímé bankovnictví | Družstevní záložny

Peníze.cz > Účty a karty > Běžné účty > Bankéři vám dají sto tisíc. Zachráníte je před piráty?

Bankéři vám dají sto tisíc. Zachráníte je před piráty?

Olga Skalková | rubrika: Aktuality | 1. 9. 2022

Zdroj: Shutterstock

Počet kybernetických útoků na klienty bank se za dva roky zvýšil čtyřnásobně, uvádí Česká bankovní asociace (ČBA). Připravila proto rozsáhlou vzdělávací kampaň s názvem #nePINdej!, kterou odstartovala právě dnes.

Na webu kybertest.cz si můžete vyzkoušet, jak jste vůči trikům podvodníkům odolní. Na začátku zábavného testu vám na virtuální účet připíšou sto tisíc korun a pak vás provádějí nejčastějšími situacemi, ve kterých jako bankovní klient můžete přijít o peníze. Pokud naletíte, peníze ztrácíte – naštěstí jen ty ve hře. Ve skutečnosti to může být mnohem nepříjemnější: průměrná škoda na jednoho poškozeného klienta podle ČBA dosáhla 161 500 korun.

Otázky kybertestu se liší podle věku, který na začátku uvedete. I praktiky hackerů jsou totiž odlišné. Test si můžete zopakovat – pokaždé se v něm objeví i nějaká

Nejnovější aktuality

15:30
Bankéři vám dají sto tisíc. Zachráníte je před piráty?

14:00
Bezvavlasy dají na burzu méně akcií. Chtěly vyšší cenu

12:50
Kvůli žádosti o přídavek na dítě už nemusíte na úřad

11:00
Kreditka Hello bank ušetří 10 % ve sportovních obchodech

31. 8.
Stoupne příspěvek na mobilitu i další

jsou totiž odlišné. Test si můžete zopakovat – pokaždé se v něm objeví i nějaká nová otázka, která v předchozím nebyla.

Pozor i na falešný příspěvek na dítě nebo úsporný tarif

Pokus o kybernetický útok podle ČBA zaznamenalo loni 81 procent finančních institucí, nejčastěji jde o phishing (podvodné e-maily, které se od klientů snaží získat jejich hesla k bankovnímu účtu) a škodlivé kódy, mířící na klienta.

„Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty (takzvaný vishing), které patří k těm nejzákeřnějším," říká výkonná ředitelka asociace Monika Zahálková. Narostlo rovněž množství podvodů na sociálních sítích. Loňskou novinkou byly takzvané reverzní inzertní podvody, kdy podvodníci oslovují prodávající na internetových bazarech a snaží se od nich získat údaje k platebním kartám:

- **Podvod na Bazoši a Sbazaru. Teď vypadá i jako kupec**

Útoky na klienty jsou stále rafinovanější a využívají nové příležitosti – policie nedávno upozornila na snahu hackerů získat od lidí Bankovní identitu pomoci nabídky na zařízení žádosti o pětitisícový příspěvek na dítě. Podobné podvody policie čeká v souvislostmi s podáváním žádosti o podporu na energie.

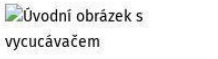
PIN nedej!

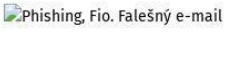
Banky se průběžně snaží informovat klienty o probíhajících kybernetických útocích. Současně opakovaně upozorňují, že přístupové údaje ke svému účtu si lidé mají chránit a neposkytovat je nikomu dalšímu. V případě pochybností mají klienti hned kontaktovat svou banku. Citlivé údaje jako jsou přístupová hesla k účtu ani banky od klientů nesmí požadovat.

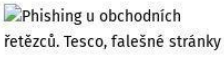
Kampaň České bankovní asociace má velké ambice, kromě asociace samotné se do ní zapojily státní i organizace a firmy: Národní úřad púro kybernetickou a informační bezpečnost (NÚKIB), dále pak Policie ČR, itego, Cisco, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy. Kampaň probíhá v médiích a na sociálních sítích, do poštovních schránek seniorů míří letáky. České dráhy je zase budou využívat třeba na papírovém prostíráních v jídelních vozech. Kampaň #nePINdej! bude trvat do prosince.

Na tohle přece neskočíte…

Otevíráme galerii skutečných pokusů o podfuk. Podívejte se, jak to může vypadat. Ale hlavně: furt ve střehu! Pořád přibývají další.







Vstoupit mezi podvodníky

Olga Skalková

O bankách a finančních institucích píše od 90. let. Byla součástí ekonomického týmu Hospodářských novin, psala i na weby iHNed.cz a Aktuálně.cz. Teď píše externě pro Peníze.cz a speciální přílohy HN. Ráda tráví čas s rodinou… Další články autora.

podpora zdravotně znevýhodněných

31. 8.
Státní zaměstnanci dostanou přidáno, potvrdila vláda

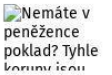
aktualizováno 31. 8.
Na energie přispějeme víc. Síkela chce trumfnout sám sebe

31. 8.
Komerční banka dá slevy na nákupy v odpovědných e-shopech

Další aktuality

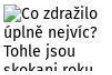
Interaktivní grafiky

Nemáte v peněžence poklad? Tyhle koruny jsou vzácné



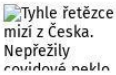
Zlatý svatováclavský pětidukát z roku 1937, který se před týdnem vydražil za rekordních…více

Co zdražilo úplně nejvíc? Tohle jsou skokani roku



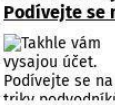
Auta. Benzin. Citrony. Droždí. Elektrika. Všecko. Zdražuje se. Ostře. Meziroční inflace…více

Tyhle řetězce mizí z Česka. Nepřežily covidové peklo



Dva roky s covidovými omezeními a uzavírkami znamenaly pohromu jak pro mnoho menších kamenných…více

Takhle vám vysajou účet. Podívejte se na triky podvodníků



Přijde e-mail, SMS, zpráva na Facebooku. Píše banka, doručovací služba nebo i finanční…více

14. #nePINdej! Počet útoků na klienty bank vzrostl, asociace spouští kampaň

Online ● idnes.cz/ekonomika (Ekonomika / Finance / Právo) ● 1. 9. 2022, 17:01

Vydavatel: **MAFRA, a.s. (cz-45313351)** ● Autor: **Sabina Ali**

Dosah: 1 434 451 ● GRP: 15.94 ● OTS: 0.16 ● AVE: 76973.61 Kč ● Interakcí: 34

Odkaz: https://www.idnes.cz/ekonomika/domaci/banky-utoky-kampan.A220901_152516_ekonomika_alis

ří 2022, svátek má Linda, Samuel

1 nová zpráva Premium

cz / ZPRAVODAJSTVÍ Domácí Zahraničí Krimi Kraje Volby Ekonomika Kultura Finance R

nika Energetická krize Daně Domácí Podniky Zahraniční Doprava Spotřebitel Test DNE

#nePINdej! Počet útoků na klienty bank vzrostl, asociace spouští kampaň

1. září 2022 17:01

Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů. Jednoho poškozeného podvodníci oberou v průměru o více než 160 tisíc korun, vyplývá z dat České bankovní asociace. Ta proto ve spolupráci s orgány státní správy a klíčovými českými firmami českého spouští rozsáhlou celonárodní vzdělávací kampaň #nePINdej!

Reklama

Ilustrační snímek | foto: Reuters

„Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším," upozornila Monika Zahálková, výkonná ředitelka České bankovní asociace.

Před dvěma lety se přitom počet takových podvodů pohyboval v nízkých stovkách, letos mluvíme již o desítkách tisíc. „Téměř každý druhý podvodný telefonát v současné době bohužel končí škodou pro klienta. Průměrné částka, o kterou klienti při těchto útocích přijdou, je přitom dost vysoká, zhruba čtvrt milionu korun," doplnila Zahálková.

Digitální doba s sebou nese rizika

Slova ředitelky ČBA potvrzuje i Lukáš Kintr, ředitel Národního úřadu pro kybernetickou a informační bezpečnost. „Žijeme v digitální době, která nám mnohé věci usnadňuje, ale také přináší rizika, a mezi ně patří i rostoucí počet různých kyberútoků. Detekujeme vysoké počty nejen podvodných telefonátů, ale i textových zpráv či emailů, a nelze očekávat, že by se jejich míra měla snižovat."

„Nejlepší obranou proti těmto pokusům nadále zůstává obecná osvěta, tedy informovanost a poučenost veřejnosti, aby byli lidé schopni vishing a podobné snahy rozpoznat," upřesňuje Kintr.

Přibývá také způsobů, jimiž se podvodníci snaží své oběti nachytat. Kromě tradičních podvodných e-mailů, SMS nebo telefonátů přibývá podvodů na sociálních sítích. V takových případech pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze.

Porazit inflaci je pro lidi složité. Doba tak přeje investičním podvodům

Novinkou loňského roku jsou takzvané reverzní inzertní podvody. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru.

„Klienti jsou oslovováni údajným kupcem jejich zboží, proto nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Chtějí zboží prodat, a tak slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně," objasnil nový trend Tomáš Kubík, náměstek policejního prezidenta pro kriminální policii.

Rozpoznat podvod pomůže kvíz

Česká bankovní asociace se proto rozhodla spustit vzdělávací kampaň, která má upozornit na sílící nebezpečí podvodů na internetu. Klíčovým prvkem kampaně #nePINdej! je interaktivní vzdělávací Kybertest, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět.

Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin.

„Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na nejstarší spoluobčany," vysvětluje Tomáš Trachta, člen představenstva společnosti Itego, která pro ČBA Kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně.

Po spuštění testu dostane každý jeho účastník virtuální peníze do „hry", které musí před podvodnými útoky co nejlépe ochránit. Po každé otázce se lidé dozvědí správné řešení, mohou se z něj tak poučit a dalšímu simulovanému útoku následně nenaletět.

„Naším cílem není lidi nachytat a ukázat jim, jak špatně se v kyberprostoru pohybují. Naším cílem je především vzdělat a naučit co nejvíce občanů, jak praktiky podvodníků odhalit a jak se nenechat hackery okrást," vysvětluje Zahálková.

Autor: alic

15. Bankéři vám dají sto tisíc. Zachráníte je před piráty?

Online ● forexbanka.cz (Ekonomika / Finance / Právo) ● 1. 9. 2022, 17:30

Vydavatel: **Ing.Josef Kadraba (cz-)** ● Autor: **Ladislav Ondra, Olga Skalková** ● Rubrika: **Akcie**

Dosah: 692 ● GRP: 0.01 ● OTS: 0.00 ● AVE: 4414.44 Kč

Odkaz: https://forexbanka.cz/bankeri-vam-daji-sto-tisic-zachranite-je-pred-piraty/

Počet kybernetických útoků na klienty bank se za dva roky zvýšil čtyřnásobně, uvádí Česká bankovní asociace (ČBA). Připravila proto rozsáhlou vzdělávací kampaň s názvem #nePINdej!, kterou odstartovala právě dnes.

Na webu kybertest.cz si můžete vyzkoušet, jak jste vůči trikům podvodníkům odolní. Na začátku zábavného testu vám na virtuální účet připíšou sto tisíc korun a pak vás provádějí nejčastějšími situacemi, ve kterých jako bankovní klient můžete přijít o peníze. Pokud naletíte, peníze ztrácíte – naštěstí jen ty ve hře. Ve skutečnosti to může být mnohem nepříjemnější: průměrná škoda na jednoho poškozeného klienta podle ČBA dosáhla 161 500 korun.

Otázky kybertestu se liší podle věku, který na začátku uvedete. I praktiky hackerů jsou totiž odlišné. Test si můžete zopakovat – pokaždé se v něm objeví i nějaká nová otázka, která v předchozím nebyla.

Pozor i na falešný příspěvek na dítě nebo úsporný tarif

Pokus o kybernetický útok podle ČBA zaznamenalo loni 81 procent finančních institucí, nejčastěji jde o phishing (podvodné e-maily, které se od klientů snaží získat jejich hesla k bankovnímu účtu) a škodlivé kódy, mířící na klienta.

„Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty (takzvaný vishing), které patří k těm nejzákeřnějším," říká výkonná ředitelka asociace Monika Zahálková. Narostlo rovněž množství podvodů na sociálních sítích. Loňskou novinkou byly takzvané reverzní inzertní podvody, kdy podvodníci oslovují prodávající na internetových bazarech a snaží se od nich získat údaje k platebním kartám:

Útoky na klienty jsou stále rafinovanější a využívají nové příležitosti – policie nedávno upozornila na snahu hackerů získat od lidí Bankovní identitu pomocí nabídky na zařízení žádosti o pětitisícový příspěvek na dítě. Podobné podvody policie čeká v souvislostmi s podáváním žádosti o podporu na energie.

PIN nedej!

Banky se průběžně snaží informovat klienty o probíhajících kybernetických útocích. Současně opakovaně upozorňují, že přístupové údaje ke svému účtu si lidé mají chránit a neposkytovat je nikomu dalšímu. V případě pochybností mají klienti hned kontaktovat svou banku. Citlivé údaje jako jsou přístupová hesla k účtu ani banky od klientů nesmí požadovat.

Kampaň České bankovní asociace má velké ambice, kromě asociace samotné se do ní zapojily státní i organizace a firmy: Národní úřad púro kybernetickou a informační bezpečnost (NÚKIB), dále pak Policie ČR, itego, Cisco, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy. Kampaň probíhá v médiích a na sociálních sítích, do poštovních schránek seniorů míří letáky. České dráhy je zase budou využívat třeba na papírovém prostírání v jídelních vozech. Kampaň #nePINdej! bude trvat do prosince.

Olga Skalková

O bankách a finančních institucích píše od 90. let. Byla součástí ekonomického týmu Hospodářských novin, psala i na weby iHNed.cz a Aktuálně.cz. Teď píše externě pro Peníze.cz a speciální přílohy HN. Ráda tráví čas s rodinou… Další články autora.
Sdílejte článek, než ho smažem

Vytisknout
Celý článek zde | Podnikání za 500 Kč ? – ANO

16. ČBA: Finanční gramotnost mírně vzrostla. Inflace ohrožuje rodinný rozpočet

Online ● opojisteni.cz (Podnikání / Marketing / PR) ● 1. 9. 2022, 17:31

Vydavatel: **oPojištění. cz s.r.o. (cz-28400887)**

Dosah: 1 652 ● GRP: 0.02 ● OTS: 0.00 ● AVE: 5456.46 Kč

Odkaz: https://www.opojisteni.cz/spektrum/cba-financni-gramotnost-mirne-vzrostla-inflace-ohrozuje-rodinny-rozpocet/c:23681/

ČBA: Finanční gramotnost mírně vzrostla. Inflace ohrožuje rodinný rozpočet

1.9.2022 **Spektrum**

Index finanční gramotnosti České bankovní asociace (ČBA) vzrostl na 56 bodů. Proti loňsku je to mírné zlepšení o jeden bod. Tři čtvrtiny dotazovaných se obávají rychlého růstu cen a kvůli současné inflaci chtějí šetřit. Velká část ale neplánuje naspořené peníze chránit proti inflačnímu znehodnocení. Přispívá k tomu i to, že se nevyznají v investicích a v radách finančních poradců. 3 z 10 rodičů budou muset omezit výdaje v souvislosti se začátkem školního roku. Vyplývá to z nového průzkumu ČBA a agentury Ipsos, který probíhal během srpna a zúčastnilo se ho 1 063 respondentů ve věku 18–79 let.

Čím vyšší vzdělání, tím lepší povědomí o financích

Částečné potíže v orientaci ve světě financí přiznává naprostá většina Čechů. Ukázaly to výsledky Indexu finanční gramotnosti, který Česká bankovní asociace dlouhodobě sleduje. Jde o sadu 11 otázek, které se týkají různých oblastí finanční gramotnosti. Největší rozdíl v úspěšnosti pozorujeme u vzdělání. Zatímco lidé s vysokoškolským vzděláním dosáhli 62 bodů, ti se základní školou nebo výučním listem získali pouze 48 bodů. Potíže přitom způsobil hlavně dotaz na výhodnost úvěru, který dokázala správně zodpovědět méně než třetina dotazovaných (31 %).

Mohlo by vás zajímat: Pod lupou Dušana Šídla: Je smrt následkem nemoci životní, nebo neživotní...

„Je vidět, že znalosti kromě vzdělání získávají lidé často i díky letitým zkušenostem. To ukazuje fakt, že lepších výsledků dosahovali lidé nad 50 let – v průměru 58 bodů. Celkově je ale pořád finanční gramotnost v Česku z mého pohledu nedostatečná a lidé selhávají v základních věcech. To má pak za následek větší zranitelnost. Česká bankovní asociace se proto snaží povědomí o financích a finančních produktech zlepšovat řadou vzdělávacích projektů. Nejoblíbenější projekty, mezi které patří Bankéři do škol a celoevropský European Money Quiz, cílí už na děti a kvůli přibývajícím kybernetickým útokům v

září startujeme velkou vzdělávací kampaň Kybertest.cz," říká Monika Zahálková výkonná ředitelka České bankovní asociace.

Za nedostatečnou finanční gramotnost může podle Čechů hlavně škola a rodina

58 % lidí si myslí, že se školy financemi ve svých vzdělávacích plánech zabývají málo nebo vůbec. Téměř třetina (32 %) je přesvědčena, že samotní učitelé nejsou dost dobře proškolení ve finančních otázkách a víc než polovina (54 %) se pak domnívá, že děti jsou k povědomí o financích nedostatečně vedeny v rodině. Z průzkumu přitom vyplývá, že na finančním vzdělávání by se měl podílet hlavně stát. Myslí si to víc než dvě třetiny dotázaných (70 %). S velkým odstupem je pak druhá v pořadí rodina, od které to čeká 30 % dotázaných. Čtvrtina z nich pak tuto roli očekává od komerčních bank a pětina od České národní banky a ministerstva financí.

Mohlo by vás zajímat: Markéta Šichtařová: Klimatologové přivolávají dluhovou krizi

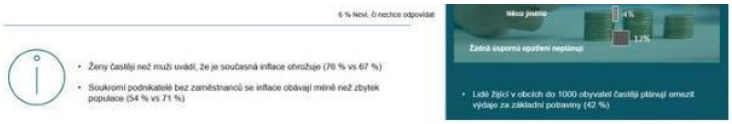
---

Jen 13 % Čechů si vždy vystačí s vlastními znalostmi

Pomoc a rady v oblasti peněz a finančních produktů častěji vyhledávají lidé s nižším vzděláním. Víc než desetina dotázaných (13 %) tvrdí, že si v této oblasti vždy vystačí se svými znalostmi. 60 % pak uvedlo, že si většinou vystačí, ale v některých případech se raději poradí s odborníkem. Často si s financemi neví rady víc než pětina respondentů, vůbec se pak v této oblasti nevyzná 6 % lidí.

Peníze si odkládá většina Čechů

Finanční rezervu nebo nějakou její formu si tvoří většina dotázaných (55 %). Nejčastěji si dávají peníze stranou na nečekané události. Polovina z nich si měsíčně odkládá do 2 500 Kč. Tyto úspory by jim nejčastěji vydržely tři měsíce. *„Já vždycky radím, aby finanční rezerva byla ve výši šestinásobku měsíčních výdajů domácnosti, a shoduji se tak s dalšími odborníky. To, že se tím podle průzkumu řídí necelá polovina obyvatel, není špatná zpráva, ale pevně věřím ve zlepšení v příštích letech,"* doplňuje Monika Zahálková.



Na důchod si lidé také odkládají stranou do 2 500 Kč, vedle finanční rezervy mají ale často i jiné zajištění v podobě domu či bytu. K dosažení svého finančního cíle polovina Čechů spoří či investuje své peníze, dvě pětiny se snaží snížit výdaje a jedna pětina hledá nový zdroj příjmů.

Mohlo by vás zajímat: Škody z povodní na menších tocích budou častější a větší

Inflace se obávají téměř tři čtvrtiny Čechů

71 % dotázaných uvádí, že inflace ohrožuje jejich rodinný rozpočet. Víc než čtvrtina přitom odpověděla, že je zdražování ohrožuje velmi. Šest z deseti respondentů si pak myslí, že jejich ekonomická situace se na konci letošního roku zhorší. I přesto 41 % oslovených lidí neplánuje své peníze před inflací chránit. Zhruba třetina (31 %) pak plánuje přesun financí na výhodné spořicí účty, 14 % chce investovat do nemovitostí, 13 % do akcií nebo dluhopisů a 9 % do zlata. Muži a lidé do 26 let častěji volí investice do akcií a dluhopisů, popřípadě do kryptoměn a NFT. Naopak lidé ve věku 54–65 let častěji neplánují žádná opatření.

„Ukazuje se, že podstatná část společnosti nevolí žádný účinný nástroj, jak ochránit své peníze před inflací. Často je to způsobeno právě i tím, že se Češi příliš nevyznají v doporučení ekonomických odborníků, případně že nerozumí investicím, které jsou jedním z nástrojů této ochrany volných finančních prostředků," doplňuje výsledky výzkumu Michal Straka, specialista na finanční trh agentury Ipsos.

Mohlo by vás zajímat: ČAP: Předpis smluvního pojistného se v 1. pololetí meziročně navýšil o 7,8 %

Děti a peníze

O penězích si s dětmi povídá většina rodičů. Nejpravidelněji o bezpečnosti nákupů na internetu a rodinných financích. 65 % rodičů pak alespoň někdy dává svým dětem do 18 let kapesné. Zřizují jim nejčastěji stavební spoření (32 %) a životní pojištění (31 %). Čtvrtina rodičů založila dětem i běžný účet, ke kterému mají vlastní platební kartu. Nejčastěji rodiče svému potomkovi zřídí účet, když je mu 10–12 let. Výjimkou ale není ani rozmezí od narození do tří let (9 %), a od čtyř do šesti let (9 %). Běžný účet má 27 % dětí, spořící účet pak 25 % z nich. 17 % rodičů uvedlo, že jejich dítě nevyužívá žádný bankovní

produkt.

58 % dětí s vlastním účtem na něj dostává od rodičů kapesné pravidelně. 41 % děti pak má na účtu další příležitostné prostředky např. od prarodičů nebo z brigád. 67 % rodičů má dohled na účtem svého dítěte, naopak 40 % rodičů uvádí, že s ním dítě může volně nakládat. Pětina lidí uvádí, že nedává dětem ani kapesné ani odměny.

3 z 10 rodičů budou muset omezit výdaje v souvislosti se začátkem školního roku

Většina rodičů, kteří uvedli, že financování školních pomůcek nezvládnou ze současných příjmů domácnosti, si nebude muset půjčovat (68 %). 32 % dotazovaných si ale bude muset vzít nějakou formu půjčky. Do 3 000 Kč si bude muset půjčit 18 % rodičů, víc než 3 000 Kč pak bude potřebovat 14 % rodičů. Omezení výdajů pak lidé spojují se zájmovými kroužky (13 %), školními aktivitami (5 %) a školními obědy (5 %). 60 % respondentů uvedlo, že nebudou muset omezit žádné aktivity.

Mohlo by vás zajímat: Pojištění proti masovému střílení v USA po vážných incidentech podražilo

Většina rodičů čeká zvýšené výdaje v souvislosti se školním rokem do 6 000 Kč

Víc než tři čtvrtiny rodičů (77 %) čekají v souvislosti se začátkem školního roku zvýšené výdaje do 6 000 Kč. Zatímco 62 % z nich vše zvládne ze současných příjmů domácnosti, 29 % využije část naspořených prostředků. Nad šesti tisícovou hranicí čeká výdaje 23 % respondentů.

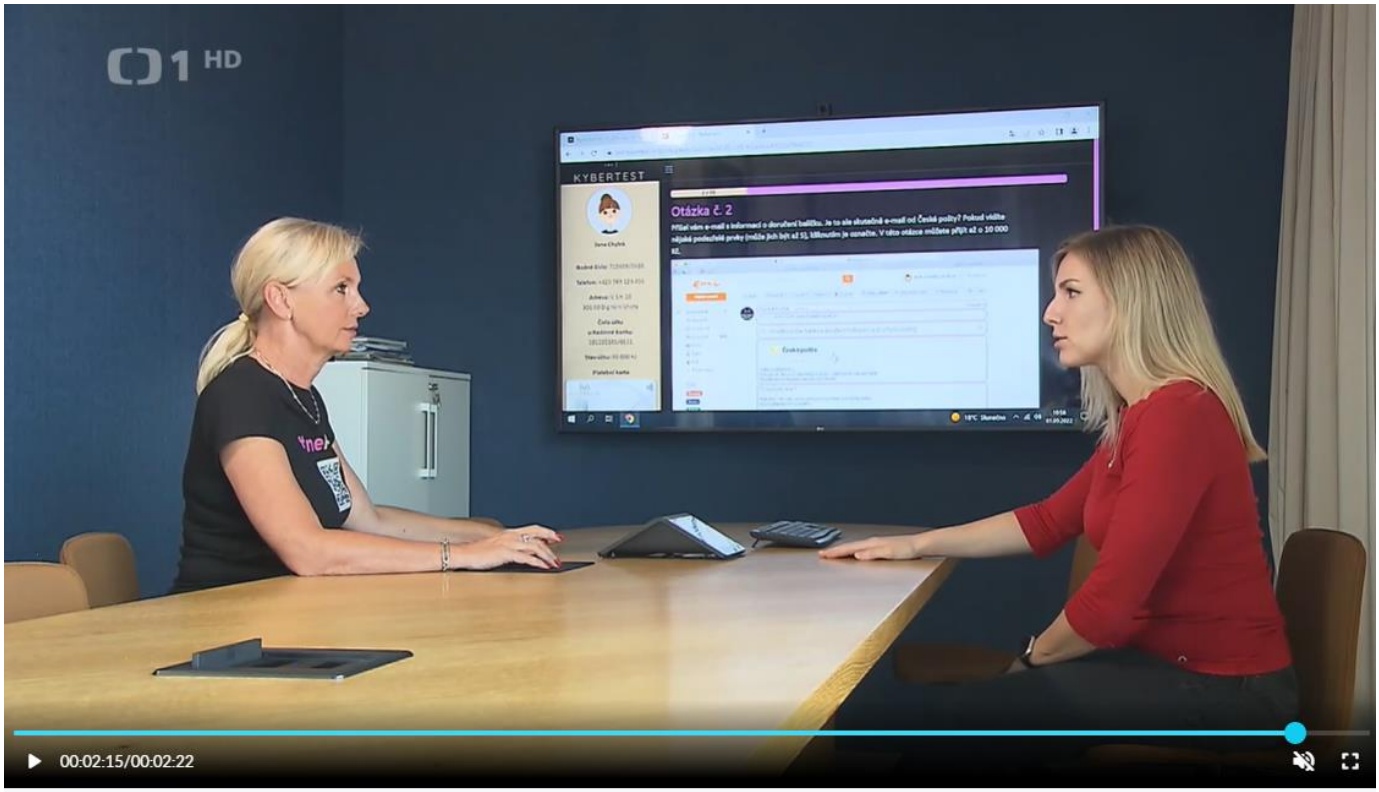
17. Podvodných útoků přibylo

Televize ● Události (ČT1) ● 1. 9. 2022, 19:47

Vydavatel: **ČESKÁ TELEVIZE (cz-00027383)**

Dosah: 609 301 ● GRP: 6.77 ● OTS: 0.07 ● AVE: 1868573.84 Kč

Odkaz: náhled



18.Startuje kampaň #nePINdej

Online ● cz-dbmonitor.echo24.cz (Zprávy / Politika) ● 1. 9. 2022, 21:20

Vydavatel: **Echo Media a.s. (cz-02581574)** ● Autor: **pp** ● Rubrika: **Homepage**

Dosah: 320 212 ● GRP: 3.56 ● OTS: 0.04 ● AVE: 45455.29 Kč

Odkaz: https://cz-dbmonitor.echo24.cz/a/S2aYf/startuje-kampan-nepindej

ECHO Monitor

Startuje kampaň #nePINdej

1. září 2022, Politika

(ČT, MFD) Počet útoků na klienty bank se za posl. 2 roky zvýšil 4x. Škody jdou do stovek mil. Kč. Dramat. narostly podvodné telefonáty, tzv. vishing, jež patří k těm nejzákeřnějším, Jednoho poškozeného podvodníci oberou v prům. o 161 500 Kč. uvádí ČBA. Asociace proto ve spolupráci s orgány státní správy a klíč. firmami spouští rozsáhlou celonár. vzdělávací kampaň #nePINdej! Klíč. prvkem kampaně je interaktivní vzdělávací Kybertest na stránkách www.kybertest.cz. Ten zábavnou formou seznámí veřejnost s nejčastějšími kybernet. podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. Nejčastější chybou lidí je, že poskytnou cizím lidem přístup. údaje ke svým účtům do mobil. či internet. bankovnictví.

Poslední zprávy z monitoringu

1. září 2022 Politika
Startuje kampaň #nePINdej

1. září 2022 Politika
Začalo Milostivé léto II

1. září 2022 Byznys
EPH a Sev.en Energy jednají se státem o úvěru

1. září 2022 Politika
Škola začala v nejistotě kvůli energiím. Přišli i politici

1. září 2022 Byznys
Šmejc kupuje rumunské sázkové kanceláře

19. Kybernetických útoků dramaticky přibývá a jsou stále rafinovanější. ČBA proto spouští celonárodní vzdělávací kampaň #nePINdej!

Online ● rizeniskoly.cz (Jiné) ● 1. 9. 2022, 21:20

Vydavatel: **Wolters Kluwer ČR, a.s. (cz-63077639)** ● Rubrika: **Aktuality**

Dosah: 606 ● GRP: 0.01 ● OTS: 0.00 ● AVE: 4098.71 Kč

Odkaz: https://www.rizeniskoly.cz/cz/aktuality/kybernetickych-utoku-dramaticky-pribyva-a-jsou-stale-rafinovanejsi-cba-proto-spousti-celonarodni-vzdelavaci-kampan-nepindej.a-8629.html

? Časté otázky | Zapomenuté heslo / Zadání nového hesla | Registrace | Přihlášení

ce Vzory Projekty Legislativa DVPP Archiv časopisů Poradna Nabídka produktů O redakci Kontakt

Vyhledávání v aktualitách ▸

HLEDAT | Rozšířené vyhledávání

30denní zkušební přístup ZDARMA

Registrace

Aktuality

Hlavní stránka

Tisk Uložit Odeslat Záložka

Kybernetických útoků dramaticky přibývá a jsou stále rafinovanější. ČBA proto spouští celonárodní vzdělávací kampaň #nePINdej!

2. 9. 2022 ▪ Kategorie: Aktuality ▪ Autor/autoři: Česká bankovní asociace

Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů a na jednoho poškozeného klienta je to v průměru 161 500 korun. Vyplynulo to z dat České bankovní asociace (ČBA), získaných od jejích členských bank. ČBA proto ve spolupráci s orgány státní správy a s klíčovými firmami českého byznysu spouští rozsáhlou celonárodní vzdělávací kampaň #nePINdej!

*„**Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším.** Zatímco před dvěma lety se jejich počet pohyboval v nízkých stovkách, letos mluvíme již o desítkách tisíc. A narostla i jejich úspěšnost. Téměř každý druhý podvodný telefonát v současné době bohužel končí škodou pro klienta. Průměrné částka, o kterou klienti při těchto útocích přijdou, je přitom dost vysoká, zhruba čtvrt milionu korun,“* uvedla **Monika Zahálková, výkonná ředitelka České bankovní asociace**. Její slova potvrzuje i **Lukáš Kintr, ředitel Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB)**. *„Žijeme v digitální době, která nám mnohé věci usnadňuje, ale také přináší mnohá rizika, a mezi ně patří i rostoucí počet různých kyberútoků. Detekujeme vysoké počty nejen podvodných telefonátů, ale i textových zpráv či e-mailů, a nelze očekávat, že by se jejich míra měla snižovat. Nejlepší obranou proti těmto pokusům nadále zůstává obecná osvěta, tedy informovanost a poučenost veřejnosti, aby byli lidé schopni vishing a podobné snahy rozpoznat,“* upřesňuje **Lukáš Kintr**.

Přibývá také způsobů, jimiž se podvodníci snaží své oběti nachytat. Kromě tradičních podvodných e-mailů, SMS a již zmíněného vishingu se stále častěji setkáváme s podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze. *„Loňskou novinkou jsou také tzv. reverzní inzertní podvody, jejichž počet neustále roste. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu‘, tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou,“* objasnil **brig. gen. Tomáš Kubík, náměstek policejního prezidenta pro kriminální policii**.

#nePINdej! – celonárodní vzdělávací kampaň v oblasti kyberbezpečnosti

Kybernetická kriminalita také již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Česká bankovní asociace proto spouští rozsáhlou vzdělávací kampaň, která má upozornit na sílící nebezpečí podvodů na internetu. Pod názvem #nePINdej! představí nejčastější kybernetické útoky a formou hravého testu na www.kybertest.cz naučí, jak jim nenaletět. Kampaní chce ČBA oslovit širokou veřejnost – mladistvé od 12 let, dospělé i seniory.

Klíčovým prvkem kampaně #nePINdej! je interaktivní vzdělávací Kybertest, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. *„Název #nePINdej! funguje jako slovní hříčka a je vtipnou výzvou, aby si lidé dávali pozor na své citlivé údaje a chránili své peníze ve světě internetu. Zároveň bude na sociálních sítích i v dalších kanálech aktivizovat veřejnost k tomu, aby si ve speciálně vytvořené online aplikaci otestovala své schopnosti obstát před kyberútoky,“* říká **Monika Zahálková, výkonná ředitelka České bankovní asociace**.

Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. *„Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na*

nejstarší spoluobčany," vysvětluje **Tomáš Trachta, člen představenstva společnosti itego, a. s.**, která pro ČBA Kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně. Po spuštění testu dostane každý jeho účastník virtuální peníze do „hry", které musí před podvodnými útoky co nejlépe ochránit. Po každé otázce se lidé dozvědí správné řešení, mohou se z něj tak poučit a dalšímu simulovanému útoku následně nenaletět. *„Naším cílem není lidi nachytat a ukázat jim, jak špatně se v kyberprostoru pohybují. Naším cílem je především vzdělat a naučit co nejvíce občanů, jak praktiky podvodníků odhalit a jak se nenechat hackery okrást,"* vysvětluje **Monika Zahálková**.

Kampaň #nePINdej! zcela jistě patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají. Kromě České bankovní asociace, která je realizátorem projektu, jsou do kampaně zapojeny Policie České republiky, Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), itego, a.s., CISCO, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy. Mediálními partnery jsou Česká televize (hlavní mediální partner), Seznam Zprávy, Deník a Cinestar.

O České bankovní asociaci

Česká bankovní asociace vznikla v roce 1990 a je dobrovolným sdružením právnických osob podnikajících v oblasti peněžnictví. V současné době sdružuje 34 členů. Rolí asociace je především zastupovat a prosazovat společné zájmy členů, prezentovat roli a zájmy bankovnictví vůči veřejnosti, podílet se na standardizaci postupů v bankovnictví a na vytváření odborných zvyklostí, podporovat harmonizaci bankovní legislativy s legislativou Evropské unie a vyvíjet aktivitu v informativní a školicí oblasti. ČBA je členem Evropské bankovní federace a EMMI. Více informací na www.cbaonline.cz.

Další dotazy zodpovíme na adrese: ***radek.salsa@cbaonline.cz***

20. Internetoví zloději zneužívají i nové příspěvky na děti

Tisk ● Klatovský deník; str. 6 (Regionální zprávy) ● 2. 9. 2022

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)**

Dosah: 333 926 ● GRP: 3.71 ● OTS: 0.04 ● AVE: 376712.72 Kč

Odkaz: náhled

6 Deník 2. září 2022
www.denik.cz

UDÁLOSTI

Krátce

Schodek rozpočtu by mohl být 270 miliard

Praha – Schodek státního rozpočtu by příští rok mohl dosáhnout 270 miliard korun. Vyplývá to z prvního návrhu rozpočtu na rok 2023, který připravilo ministerstvo financí. Návrh počítá s příjmy 1,749 bilionu Kč a výdaji 2,019 bilionu Kč. **(čtk)**

Americký ministr obrany bude jednat s Fialou

Praha – Příští pátek do Česka přiletí americký ministr obrany Lloyd Austin. Bude v Praze jednat s ministryní obrany Janou Černochovou i s premiérem Petrem Fialou (oba ODS). Tématem bude pomoc Ukrajině nebo aktuální bezpečnostní situace. Česká republika má mimo jiné zájem o nákup amerických stíhacích letounů F-35. **(čtk)**

Benzin i nafta zdražují

Praha – Po dvou měsících poklesu vzrostla průměrná cena benzinu Natural 95 u čerpacích stanic v Česku v uplynulém týdnu o 22 haléřů na 40,54 koruny za litr. Litr nafty stál ve středu v průměru 45,23 korun, cena tak za týden vyskočila o 2,37 koruny. Vyplývá to z údajů společnosti CCS. Podle analytiků bude nafta ještě zdražovat, cena benzinu by měla stagnovat. „Významným problémem pro celou Evropu je prudký růst velkoobchodních marží u nafty na 60 dolarů (zhruba 1470 Kč) za barel z 30 dolarů (735 Kč) v polovině srpna. U benzinu se marže drží na 13 dolarech (zhruba 320 Kč) za barel. Prudké zvýšení velkoobchodních cen se ještě nedokázalo plně promítnout do maloobchodních cen. Nafta proto zdraží ještě o několik desítek haléřů," uvedl analytik společnosti Finlord Boris Tomčiak. **(čtk)**

Už zítra v Deníku

ČTĚTE V SOBOTNÍM VYDÁNÍ MAGAZÍNU **VÍKEND**:

Zuzana Lapčíková: Učení je koníček

HVĚZDA. Cimbalistka a zpěvačka Zuzana Lapčíková už po několik desetiletí symbolizuje spojení moravské lidové hudby a jazzu. Půvabná, svěží dáma je rovněž matkou tří dětí a kromě neustálého hraní doma i v zahraničí působí jako pedagožka na soukromé Základní umělecké škole ve Zlíně. Učení má podle svých slov jako aristokratického koníčka.

NA KOLE PODÉL LABE. Osm set padesát dva kilometrů. Tolik dělí českou hranici u Hřenska od ústí Labe do Severního moře. Cesta Německem, východním, západním a severním, trvala redaktorovi Deníku Luboši Palatovi skoro tři týdny. Byly to ale prý jedny z nejhezčích tří týdnů v jeho životě.

NÁVŠTĚVA NEW YORKU. Jedno z nejrušnějších měst světa. Tím je rozhodně americký New York, který se po covidu stal opět tepající metropolí plnou zábavy. Co lze v New Yorku zažít? Tak samozřejmě lze vystát nesmyslně dlouhou frontu, zaplatit nesmyslně vysoký poplatek a nechat se dovézt k soše Svobody, kde se dozvíte její historii. Anebo můžete zažít New York jinak, mnohem levněji, a přesto vzrušujícím způsobem.

TŘEBÍZSKÉHO KLEČANY. Asi pět kilometrů severně od Prahy na skále nad řekou Vltavou se rozprostírá starobylá obec Klecany. Mají tu hostel Nanebevzetí Panny Marie, kde působil jako kaplan spisovatel historických próz Václav Beneš Třebízský.

Magazín Víkend. Již zítra ve vašem Deníku

Přehledně: Do konce roku se otevře 26 kilometrů dálnic

www.denik.cz

Dokončení ze str. 1

Dálniční síť v Česku měřící zhruba 1350 kilometrů se rozšíří do konce roku o více než dvě desítky nových kilometrů. Stát ze ně celkově zaplatí zhruba osm miliard korun. Nejdelší úsek přibude na dálnici D35, tedy hlavní spojnici Čech a Moravy.

První úseky nových autostrád u Frýdku-Místku se otevřou už dnes, zbylé postupně v posledním čtvrtletí letošního roku. Větší rozmach dálnic se očekává až za dva roky.

STOVKY NOVÝCH KILOMETRŮ

V současné době je ve výstavbě zhruba dvě stě čtyřicet kilometrů dálnic a silnic I. třídy. „Dálnic na zelené louce je rozestavěno 150,6 kilometru," uvedlo ministerstvo dopravy. Staví se mimo jiné na dálnici D4 mezi Příbrami a Pískem či na D3 ve směru od Českých Budějovic k hranicím s Rakouskem. Zatímco za letošek celkem přibude necelých šestadvacet kilometrů dálnic, v příštím silničáři dokončí ještě o šest kilometrů dálnic víc.

V roce 2024 by to pak měla být dokonce další skoro stovka kilometrů, což by byl rekordní nárůst. Až doposud bylo v Česku, respektive v Československu, v jednom roce zprovozněno maximálně osmasedmdesát nových kilometrů, a to v letech 1980 a 2006. Naopak před čtyřmi lety se dálniční síť zvětšila o pouhé čtyři kilometry.

Internetoví zloději zneužívají i nové příspěvky na děti

VILÉM JANOUŠ

Kriminalita se přesouvá do virtuálního světa a zloději touží po účtech klientů bank. Škody jdou do stovek milionů, přičemž na jednoho poškozeného připadá částka přes 160 tisíc korun. Česká bankovní asociace se rozhodla bránit. Chce učit lidi, jak podvodníkům nenaletět.

„Pokud se necháte na internetu napálit, téměř jistě své penize už neuvidíte. Když budete mít štěstí, vrátí se vám jejich menší část," uvedl náměstek policejního prezidenta Tomáš Kubík.

Upozornil, že počet trestných činů na internetu roste, stejně jako počet kybernetických podvodníků.

Ti se nedávno snažili získat data příjemců pětitisícového příspěvku na děti. „Lidem chodily podvodné textové zprávy, aby poskytli data ke svým účtům s tím, že jim pak budou příspěvky chodit automaticky," uvedla výkonná ředitelka České bankovní asociace Monika Zahálková. Data ale záškodníci využili k vysátí účtů poškozených.

„Naivní je si myslet, že když nic nemám na účtu, nemůžu o nic přijít."
náměstek policejního prezidenta Tomáš Kubík

Vzrůstající aktivitu zločinců na síti dokládají také nejnovější čísla. „Jen za posledních sedm měsíců byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Narostly hlavně podvodné telefonáty," řekla Zahálková.

Náměstek policejního prezidenta Kubík varoval, že pachatelé jsou sociální inženýři, kteří vědí, na jakou skupinu lidí se zaměřit. Navní je si myslet, že když nic nemám na účtu, nemůžu o nic přijít. Jakmile dám někomu své údaje, je možné si jejich prostřednictvím třeba sjednat úvěr," popsal.

Bankovní asociace proto rozjela kampaň s názvem #nePINdej!, která má na nebezpečí na internetu upozorňovat. Je zaměřená na mladé i starší. Na adrese www.kybertest.cz si lidé mohou osvojit dovednosti, jak internetovým zlodějům nenaletět. Na internetové podvody se zaměří také připravovaný seriál Deníku, který na stránkách novin najdete ještě v září.

PRAŽSKÝ deník

První profesionální hasička slouží v Praze

ELIŠKA STODOLOVÁ

Praha – Hasičský záchranný sbor v pražských Holešovicích má ve svých řadách první profesionálku, která bude sloužit ve výjezdové jednotce. Je jí dvaatřicetiletá Michaela Žďárská, která dříve sloužila u dobrovolných hasičů. U profesionálů přitom dodnes slouží jen jen na operačních středisích nebo na odboru prevence. „Celkem máme 10 550 profesionálních hasičů a z toho 969 žen. Žádná ale neslouží na výjezdu," říká generální ředitel hasičského záchranného sboru Vladimír Vlček, který věří, že přijetí Žďárské otevře dveře i dalším ženám.

Dvaatřicetiletá Michaela vystudovala střední školu s maturitou zaměřenou na cestovní ruch. Před třemi lety se po přestěhování do Dolních Měcholup přihlásila na inzerát, který nabízel místo u dobrovolných hasičů. „Splnila jsem podmínky. Bylo mi více než sedmnáct let a byla jsem fyzicky zdatná," vzpomíná.

Od té doby se nepovečená profesionální hasička zúčastnila u dobrovolných hasičů necelých padesáti výjezdů. Jako nejnáročnější zásah uvádí loňský požár bytu v Černokostelecké ulici. Mezi čtrnácti popálenými bylo i sedm dětí. „Z psychologického hlediska považuji za svou výhodu právě ženskou empatii. Především pro děti může být ženský hlas při zásahu příjemnější," říká.

Mužského kolektivu v profesionální hasičské výjezdové jednotce, sídlící v pražských Holešovicích, se prý nebojí. „První směnu mám až v sobotu. Nicméně u dobrovolných hasičů je to v pořádku, tam jsme si na sebe zvykli a jsme sžití," popisuje Žďárská a dodává, že má ráda černý humor, který je mezi hasiči rozšířený.

Vlček přiznává, že takové prostředí nemusí být pro ženu jednoduché. „Stávající osazenstvo sboru je velmi maskulinní a do sebe uzavřené," dodal.

Holešovická hasičská stanice nebyla vybraná náhodou. Díky rekonstrukci, která byla dokončena na přelomu roku, má potřebné hygienické zázemí a prostor pro oddělenou šatnu. Ve starších stanicích by právě tento požadavek mohl být problémem.

21. Kybernetických útoků dramaticky přibývá a jsou stále rafinovanější

Online ● vecerni-praha.cz (Regionální zprávy) ● 2. 9. 2022, 8:09

Vydavatel: **Stellar Media s.r.o. (cz-17187532)**

Dosah: 10 881 ● GRP: 0.12 ● OTS: 0.00 ● AVE: 2000.00 Kč ● Interakcí: 10

Odkaz: https://www.vecerni-praha.cz/kybernetickych-utoku-dramaticky-pribyva-a-jsou-stale-rafinovanejsi/

NOVÁ VEČERNÍ PRAHA

Noviny pro Prahu a okolí, denní

Z domova | Ze světa | Ekonomika | Bydlení | Auto-moto | Tech | Cestování | Gastro | Kultura

NEXT STORY
českého chřestu prodal Lidl

PREVIOUS STORY
statkové IT odborníky si v
ssu vychovávají interně

DOMOVA
Nejvíce českého chřestu prodal Lidl
2.9.2022
Letošní ocenění za největší rodaného českého chřestu idlu. V průběhu […]

Kybernetických útoků dramaticky přibývá a jsou stále rafinovanější
2.9.2022
á na klienty bank se za poslední ýšil čtyřnásobně. Škody jdou do

Nedostatkové IT odborníky si v Nessu vychovávají interně
2.9.2022
Nedostatek potřebných IT řeší rostoucí počet IT firem dí bez […]

20° C H: +21° L: +11°
Praha
Pátek, 02 Září
Viz 7denní předpověď
po út st čt

Z DOMOVA

Kybernetických útoků dramaticky přibývá a jsou stále rafinovanější

BY REDAKCE · 2.9.2022

Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů a na jednoho poškozeného klienta je to v průměru 161 500 korun. Vyplynulo to z dat České bankovní asociace (ČBA), získaných od jejích členských bank. ČBA proto ve spolupráci s orgány státní správy a s klíčovými firmami českého byznysu spouští rozsáhlou celonárodní vzdělávací kampaň #nePINdej!

„Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším. Zatímco před dvěma lety se jejich počet pohyboval v nízkých stovkách, letos mluvíme již o desítkách tisíc. A narostla i jejich úspěšnost. Téměř každý druhý podvodný telefonát v současné době bohužel končí škodou pro klienta. Průměrné částka, o kterou klienti při těchto útocích přijdou, je přitom dost vysoká, zhruba čtvrt milionu korun,“ uvedla **Monika Zahálková,** výkonná ředitelka České bankovní asociace. Její slova potvrzuje i **Lukáš Kintr,** ředitel Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). *„Žijeme v digitální době, která nám mnohé věci usnadňuje, ale také přináší mnohá rizika, a mezi ně patří i rostoucí počet různých kyberútoků. Detekujeme vysoké počty nejen podvodných telefonátů, ale i textových zpráv či e-mailů, a nelze očekávat, že by se jejich míra měla snižovat. Nejlepší obranou proti těmto pokusům nadále zůstává obecná osvěta, tedy informovanost a poučenost veřejnosti, aby byli lidé schopni vishing a podobné snahy rozpoznat,“* upřesňuje **Lukáš Kintr**.

Přibývá také způsobů, jimiž se podvodníci snaží své oběti nachytat

Přibývá také způsobů, jimiž se podvodníci snaží své oběti nachytat. Kromě tradičních podvodných e-mailů, SMS a již zmíněného vishingu se stále častěji setkáváme s podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze. *„Loňskou novinkou jsou také tzv. reverzní inzertní podvody, jejichž počet neustále roste. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou,"* objasnil **brig. gen. Tomáš Kubík,** náměstek policejního prezidenta pro kriminální policii.

#nePINdej! – celonárodní vzdělávací kampaň v oblasti kyberbezpečnosti

Kybernetická kriminalita také již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Česká bankovní asociace proto spouští rozsáhlou vzdělávací kampaň, která má upozornit na sílící nebezpečí podvodů na internetu. Pod názvem #nePINdej! představí nejčastější kybernetické útoky a formou hravého testu na www.kybertest.cz naučí, jak jim nenaletět. Kampaní chce ČBA oslovit širokou veřejnost – mladistvé od 12 let, dospělé i seniory.

Klíčovým prvkem kampaně #nePINdej! je interaktivní vzdělávací Kybertest, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. *„Název #nePINdej! funguje jako slovní hříčka a je vtipnou výzvou, aby si lidé dávali pozor na své citlivé údaje a chránili své peníze ve světě internetu. Zároveň bude na sociálních sítích i v dalších kanálech aktivizovat veřejnost k tomu, aby si ve speciálně vytvořené online aplikaci otestovala své schopnosti obstát před kyberútoky,"* říká **Monika Zahálková,** výkonná ředitelka České bankovní asociace.

Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. *„Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na nejstarší spoluobčany,"* vysvětluje **Tomáš Trachta,** člen představenstva společnosti itego, a.s., která pro ČBA Kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně. Po spuštění testu dostane každý jeho účastník virtuální peníze do „hry", které musí před podvodnými útoky co nejlépe ochránit. Po každé otázce se lidé dozvědí správné řešení, mohou se z něj tak poučit a dalšímu simulovanému útoku následně nenaletět. *„Naším cílem není lidi nachytat a ukázat jim, jak špatně se v kyberprostoru pohybují. Naším cílem je především vzdělat a naučit co nejvíce občanů, jak praktiky podvodníků odhalit a jak se nenechat hackery okrást,"* vysvětluje **Monika Zahálková**.

Kampaň #nePINdej! zcela jistě patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají. Kromě České bankovní asociace, která je realizátorem projektu, jsou do kampaně zapojeny Policie České republiky, Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), itego, a.s., CISCO, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy. Mediálními partnery jsou Česká televize (hlavní mediální partner), Seznam Zprávy, Deník a Cinestar

22. ČBA spouští vzdělávací kampaň #nePINdej!

Online ● expressauto.cz (Průmysl / Logistika) ● 2. 9. 2022, 8:54

Vydavatel: **Ing. Erich Handl (cz-71304231)** ● Rubrika: **Banky**

Dosah: 12 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 750.33 Kč

Odkaz: https://www.expressauto.cz/cba-spousti-vzdelavaci-kampan-nepindej/

Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů a na jednoho poškozeného klienta je to v průměru 161 500 korun. Vyplynulo to z dat České bankovní asociace (ČBA). ČBA proto ve spolupráci s orgány státní správy a s klíčovými firmami českého byznysu spouští celonárodní vzdělávací kampaň #nePINdej!

„Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším. Zatímco před dvěma lety se jejich počet pohyboval v nízkých stovkách, letos mluvíme již o desítkách tisíc. A narostla i jejich úspěšnost.

Téměř každý druhý podvodný telefonát v současné době bohužel končí škodou pro klienta. Průměrné částka, o kterou klienti při těchto útocích přijdou, je přitom dost vysoká, zhruba čtvrt milionu korun," uvedla Monika Zahálková, výkonná ředitelka České bankovní asociace. Její slova potvrzuje i Lukáš Kintr, ředitel Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

„Žijeme v digitální době, která nám mnohé věci usnadňuje, ale také přináší mnohá rizika, a mezi ně patří i rostoucí počet různých kyberútoků. Detekujeme vysoké počty nejen podvodných telefonátů, ale i textových zpráv či e-mailů, a nelze očekávat, že by se jejich míra měla snižovat. Nejlepší obranou proti těmto pokusům nadále zůstává obecná osvěta, tedy informovanost a poučenost veřejnosti, aby byli lidé schopni vishing a podobné snahy rozpoznat," upřesňuje Lukáš Kintr.

Přibývá také způsobů, jimiž se podvodníci snaží své oběti nachytat. Kromě tradičních podvodných e-mailů, SMS a již zmíněného vishingu se stále častěji setkáváme s podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze.

„Loňskou novinkou jsou také tzv. reverzní inzertní podvody, jejichž počet neustále roste. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou," objasnil brig. gen. Tomáš Kubík, náměstek policejního prezidenta pro kriminální policii.

#nePINdej! – celonárodní vzdělávací kampaň v oblasti kyberbezpečnosti

#nePINdej!

Kybernetická kriminalita také již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Česká bankovní asociace proto spouští rozsáhlou vzdělávací kampaň, která má upozornit na sílící nebezpečí podvodů na internetu. Pod názvem #nePINdej! představí nejčastější kybernetické útoky a formou hravého testu na

www.kybertest.cz naučí, jak jim nenaletět. Kampaní chce ČBA oslovit širokou veřejnost – mladistvé od 12 let, dospělé i seniory.

Klíčovým prvkem kampaně #nePINdej! je interaktivní vzdělávací Kybertest, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. *„Název #nePINdej! funguje jako slovní hříčka a je vtipnou výzvou, aby si lidé dávali pozor na své citlivé údaje a chránili své peníze ve světě internetu. Zároveň bude na sociálních sítích i v dalších kanálech aktivizovat veřejnost k tomu, aby si ve speciálně vytvořené online aplikaci otestovala své schopnosti obstát před kyberútoky,"* říká **Monika Zahálková, výkonná ředitelka České bankovní asociace**.

Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. *„Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na nejstarší spoluobčany,"* vysvětluje **Tomáš Trachta, člen představenstva společnosti itego, a.s.**, která pro ČBA Kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně. Po spuštění testu dostane každý jeho účastník virtuální peníze do „hry", které musí před podvodnými útoky co nejlépe ochránit. Po každé otázce se lidé dozvědí správné řešení, mohou se z něj tak poučit a dalšímu simulovanému útoku následně nenaletět. *„Naším cílem není lidi nachytat a ukázat jim, jak špatně se v kyberprostoru pohybují. Naším cílem je především vzdělat a naučit co nejvíce občanů, jak praktiky podvodníků odhalit a jak se nenechat hackery okrást,"* vysvětluje **Monika Zahálková**.

Kampaň #nePINdej! zcela jistě patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají. Kromě České bankovní asociace, která je realizátorem projektu, jsou do kampaně zapojeny Policie České republiky, Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), itego, a.s., CISCO, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy. Mediálními partnery jsou Česká televize (hlavní mediální partner), Seznam Zprávy, Deník a Cinestar.

Zdroj: TK ČBA

Kortus

2.září 2022

23. ČBA spouští vzdělávací kampaň #nePINdej!

Online ● czechbanking.cz (Ekonomika / Finance / Právo) ● 2. 9. 2022, 9:20

Vydavatel: **Ing. Erich Handl (cz-71304231)**

Dosah: 8 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 750.00 Kč

Odkaz: https://www.czechbanking.cz/cba-spousti-vzdelavaci-kampan-nepindej/

Vyplynulo to z dat České bankovní asociace (ČBA), získaných od jejích členských bank. ČBA proto ve spolupráci s orgány státní správy a s klíčovými firmami českého byznysu spouští rozsáhlou celonárodní vzdělávací kampaň #nePINdej!

„Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším. Zatímco před dvěma lety se jejich počet pohyboval v nízkých stovkách, letos mluvíme již o desítkách tisíc. A narostla i jejich úspěšnost. Téměř každý druhý podvodný telefonát v současné době bohužel končí škodou pro klienta. Průměrné částka, o kterou klienti při těchto útocích přijdou, je přitom dost vysoká, zhruba čtvrt milionu korun," uvedla Monika Zahálková, výkonná ředitelka České bankovní asociace. Její slova potvrzuje i Lukáš Kintr, ředitel Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). „Žijeme v digitální době, která nám mnohé věci usnadňuje, ale také přináší mnohá rizika, a mezi ně patří i rostoucí počet různých kyberútoků. Detekujeme vysoké počty nejen podvodných telefonátů, ale i textových zpráv či e-mailů, a nelze očekávat, že by se jejich míra měla snižovat. Nejlepší obranou proti těmto pokusům nadále zůstává obecná osvěta, tedy informovanost a poučenost veřejnosti, aby byli lidé schopni vishing a podobné snahy rozpoznat," upřesňuje Lukáš Kintr.

Přibývá také způsobů, jimiž se podvodníci snaží své oběti nachytat. Kromě tradičních podvodných e-mailů, SMS a již zmíněného vishingu se stále častěji setkáváme s podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze. „Loňskou novinkou jsou také tzv. reverzní inzertní podvody, jejichž počet
ustále roste. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako
tební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím
něženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží,
předpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového
nkovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují
aje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají
níze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou," objasnil brig. gen. Tomáš Kubík, náměstek policejního prezidenta pro kriminální policii.

#nePINdej! – celonárodní vzdělávací kampaň v oblasti kyberbezpečnosti

Kybernetická kriminalita také již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Česká bankovní asociace proto spouští rozsáhlou vzdělávací kampaň, která má upozornit na sílící nebezpečí podvodů na internetu. Pod názvem #nePINdej! představí nejčastější kybernetické útoky a formou hravého testu na www.kybertest.cz naučí, jak jim nenaletět. Kampaní chce ČBA oslovit širokou veřejnost – mladistvé od 12 let, dospělé i seniory.

Klíčovým prvkem kampaně #nePINdej! je interaktivní vzdělávací Kybertest, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. *„Název #nePINdej! funguje jako slovní hříčka a je vtipnou výzvou, aby si lidé dávali pozor na své citlivé údaje a chránili své peníze ve světě internetu. Zároveň bude na sociálních sítích i v dalších kanálech aktivizovat veřejnost k tomu, aby si ve speciálně vytvořené online aplikaci otestovala své schopnosti obstát před kyberútoky,"* říká **Monika Zahálková, výkonná ředitelka České bankovní asociace**.

Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. *„Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na nejstarší spoluobčany,"* vysvětluje **Tomáš Trachta, člen představenstva společnosti itego, a.s.**, která pro ČBA Kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně. Po spuštění testu dostane každý jeho účastník virtuální peníze do „hry", které musí před podvodnými útoky co nejlépe ochránit. Po každé otázce se lidé dozvědí správné řešení, mohou se z něj tak poučit a dalšímu simulovanému útoku následně nenaletět. *„Naším cílem není lidi nachytat a ukázat jim, jak špatně se v kyberprostoru pohybují. Naším cílem je především vzdělat a naučit co nejvíce občanů, jak praktiky podvodníků odhalit a jak se nenechat hackery okrást,"* vysvětluje **Monika Zahálková**.

Kampaň #nePINdej! zcela jistě patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají. Kromě České bankovní asociace, která je realizátorem projektu, jsou do kampaně zapojeny Policie České republiky, Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), itego, a.s., CISCO, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy. Mediálními partnery jsou Česká televize (hlavní mediální partner), Seznam Zprávy, Deník a Cinestar.

24. ČBA spouští vzdělávací kampaň #nePINdej!

Online ● autologistika.cz (Průmysl / Logistika) ● 2. 9. 2022, 9:51

Vydavatel: **Ing. Erich Handl (cz-71304231)**

Dosah: 52 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 1002.99 Kč

Odkaz: https://www.autologistika.cz/cba-spousti-vzdelavaci-kampan-nepindej/

stovek milionů a na jednoho poškozeného klienta je to v průměru 101 500 korun. Vyplynulo to z dat České bankovní asociace (ČBA). ČBA proto ve spolupráci s orgány státní správy a s klíčovými firmami českého byznysu spouští celonárodní vzdělávací kampaň #nePINdej!

„Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším. Zatímco před dvěma lety se jejich počet pohyboval v nízkých stovkách, letos mluvíme již o desítkách tisíc. A narostla i jejich úspěšnost.

Téměř každý druhý podvodný telefonát v současné době bohužel končí škodou pro klienta. Průměrné částka, o kterou klienti při těchto útocích přijdou, je přitom dost vysoká, zhruba čtvrt milionu korun," uvedla Monika Zahálková, výkonná ředitelka České bankovní asociace. Její slova potvrzuje i Lukáš Kintr, ředitel Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

„Žijeme v digitální době, která nám mnohé věci usnadňuje, ale také přináší mnohá rizika, a mezi ně patří i rostoucí počet různých kyberútoků. Detekujeme vysoké počty nejen podvodných telefonátů, ale i textových zpráv či e-mailů, a nelze očekávat, že by se jejich míra měla snižovat. Nejlepší obranou proti těmto pokusům nadále zůstává obecná osvěta, tedy informovanost a poučenost veřejnosti, aby byli lidé schopni vishing a podobné snahy rozpoznat," upřesňuje Lukáš Kintr.

Přibývá také způsobů, jimiž se podvodníci snaží své oběti nachytat. Kromě tradičních podvodných e-mailů, SMS a již zmíněného vishingu se stále častěji setkáváme s podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze.

ňskou novinkou jsou také tzv. reverzní inzertní podvody, jejichž počet neustále roste. Terčem čníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu zpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného zaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich kdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem ží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a stupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou," objasnil brig. gen. Tomáš Kubík, náměstek policejního prezidenta pro kriminální policii.

#nePINdej! – celonárodní vzdělávací kampaň v oblasti kyberbezpečnosti

Kybernetická kriminalita také již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Česká bankovní asociace proto spouští rozsáhlou vzdělávací kampaň, která má upozornit na sílící nebezpečí podvodů na internetu. Pod názvem #nePINdej! představí nejčastější kybernetické útoky a formou hravého testu na www.kybertest.cz naučí, jak jim nenaletět. Kampaní chce ČBA oslovit širokou veřejnost – mladistvé od 12 let, dospělé i seniory.

Klíčovým prvkem kampaně #nePINdej! je interaktivní vzdělávací Kybertest, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. *„Název #nePINdej! funguje jako slovní hříčka a je vtipnou výzvou, aby si lidé dávali pozor na své citlivé údaje a chránili své peníze ve světě internetu. Zároveň bude na sociálních sítích i v dalších kanálech aktivizovat veřejnost k tomu, aby si ve speciálně vytvořené online aplikaci otestovala své schopnosti obstát před kyberútoky,"* říká **Monika Zahálková, výkonná ředitelka České bankovní asociace**.

Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. *„Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na nejstarší spoluobčany,"* vysvětluje **Tomáš Trachta, člen představenstva společnosti itego, a.s.**, která pro ČBA Kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně. Po spuštění testu dostane každý jeho účastník virtuální peníze do „hry", které musí před podvodnými útoky co nejlépe ochránit. Po každé otázce se lidé dozvědí správné řešení, mohou se z něj tak poučit a dalšímu simulovanému útoku následně nenaletět. *„Naším cílem není lidi nachytat a ukázat jim, jak špatně se v kyberprostoru pohybují. Naším cílem je především vzdělat a naučit co nejvíce občanů, jak praktiky podvodníků odhalit a jak se nenechat hackery okrást,"* vysvětluje **Monika Zahálková**.

Kampaň #nePINdej! zcela jistě patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají. Kromě České bankovní asociace, která je realizátorem projektu, jsou do kampaně zapojeny Policie České republiky, Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), itego, a.s., CISCO, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy. Mediálními partnery jsou Česká televize (hlavní mediální partner), Seznam Zprávy, Deník a Cinestar.

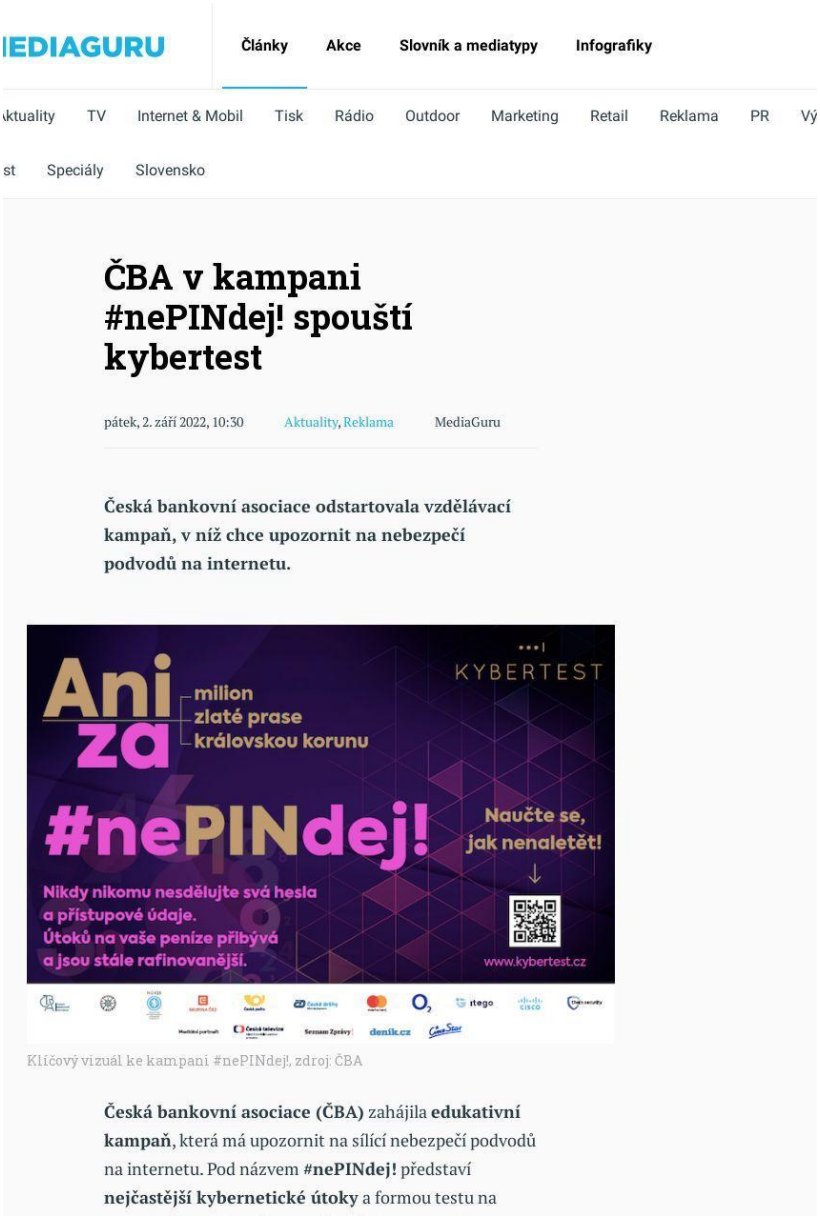
25. ČBA v kampani #nePINdej! spouští kybertest

Online ● mediaguru.cz (Podnikání / Marketing / PR) ● 2. 9. 2022, 10:30

Vydavatel: **PHD, a.s. (cz-26210738)**

Dosah: 4 273 ● GRP: 0.05 ● OTS: 0.00 ● AVE: 12226.99 Kč

Odkaz: https://www.mediaguru.cz/clanky/2022/09/cba-v-kampani-nepindej-spousti-kybertest/



www.kybertest.cz chce naučit, jak jim nenaletět. Kampaní cílí na širokou veřejnost – mladistvé od 12 let, dospělé i seniory.

„Počet kybernetických podvodů dramaticky roste a vyvíjejí se i metody útočníků. Česká bankovní asociace proto startuje rozsáhlou celonárodní kybernetickou kampaň, která se zaměřuje na širokou veřejnost od teenagerů až po seniory. Na každou cílovou skupinu přitom míříme jinými komunikačními kanály, protože chceme, aby byla kampaň co nejefektivnější a oslovila opravdu každého," říká výkonná ředitelka České bankovní asociace **Monika Zahálková**.

Klíčovým prvkem kampaně je již zmíněný kybertest s několika variantami, které simulují nejčastější podvodné praktiky dle různých věkových skupin. „Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na nejstarší spoluobčany," vysvětluje **Tomáš Trachta** ze společnosti **Itego,** která pro ČBA kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně.

Kampaň bude probíhat napříč všemi médii – **na internetu, v tisku, v televizi, formou letáků** na pobočkách České pošty, **ve vlacích a na nádražích** Českých drah, ale i **na bankomatech** bank působících na českém trhu. Součástí budou i **SMS** zprávy od společnosti O2, které vyzvou k účasti na testu. Ze **sociálních sítí** bude kromě Facebooku, LinkedInu, Twitteru, a Instagramu využit i TikTok. Kampaň podpoří na svých profilech i influencer **Martin „Mikýř" Mikyska**.

Cílit bude kampaň však i na tu část veřejnosti, která se na internetu pohybuje sporadicky nebo vůbec. „Ač se to může zdát zvláštní, i tato část populace je ohrožena kyberútoky, a to ve formě podvodných telefonátů. Proto ji nemůžeme opominout. Připravili jsme pro ni speciální letáky, které budou distribuovány Českou poštou nebo obcemi s rozšířenou působností," dodává **Monika Zahálková** a doplňuje: „Během podzimu bychom také rádi pronikli i na druhý stupeň základních škol a do

středních škol, a to formou kyberhry. Bude to podobná forma testu, jen přímo šitá na míru nejmladší generaci, která již může mít vlastní bankovní účet."

„Název kampaně #nePINdej! funguje jako slovní hříčka a je vtipnou výzvou, aby si lidé dávali pozor na své citlivé údaje a chránili své peníze ve světě internetu," popisuje **Marek Pražák** z agentury **Svengali Communication**, která je autorem kreativní idey a realizátorem kampaně na sociálních sítích.

Vizuálně se chce kampaň od ostatních podobných kampaní odlišit tím, že na první pohled nedělí. „Většina kampaní varujících před kyberpodvodníky využívá ve vizuálech obrázky hackera nebo jiné výstražné symboly. My jsme na to chtěli jít jinak – chceme upoutat pozornost nejen claimem #nePINdej!, ale i barvami, které jsou výrazné, ale příjemné a neděsí. Nechceme v kampani pracovat s pocitem strachu, ale spíš nalákat lidi na hru, díky níž se naučí, jak útočníkům nenaletět," dodává **Petr Martinovský** ze společnosti DTPak.cz, která je autorem vizuálního zpracování kampaně.

Do kampaně se zapojily jak **orgány státní správy**, které se kyberbezpečností zabývají, tak **klíčové firmy českého byznysu**, jichž samotných nebo jejich klientů se podvodné útoky také týkají. Kromě České bankovní asociace, která je realizátorem projektu, jsou do kampaně zapojeny Policie České republiky, Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), Itego, CISCO, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy. Mediálními partnery jsou Česká televize, Seznam Zprávy a Deník.

-stk-

26. Kybernetických útoků dramaticky přibývá a jsou stále rafinovanější

Online ● poradci-sobe.cz (Podnikání / Marketing / PR) ● 2. 9. 2022, 13:34

Vydavatel: **4stones, s.r.o. (cz-29002303)**

Dosah: 989 ● GRP: 0.01 ● OTS: 0.00 ● AVE: 5353.70 Kč

Odkaz: https://poradci-sobe.cz/informacni-servis/kybernetickych-utoku-dramaticky-pribyva-a-jsou-stale-rafinovanejsi/

Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů a na jednoho poškozeného klienta je to v průměru 161 500 korun. Vyplynulo to z dat České bankovní asociace (ČBA), získaných od jejích členských bank. ČBA proto ve spolupráci s orgány státní správy a s klíčovými firmami českého byznysu spouští rozsáhlou celonárodní vzdělávací kampaň #nePINdej!

„Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším. Zatímco před dvěma lety se jejich počet pohyboval v nízkých stovkách, letos mluvíme již o desítkách tisíc. A narostla i jejich úspěšnost. Téměř každý druhý podvodný telefonát v současné době bohužel končí škodou pro klienta. Průměrné částka, o kterou klienti při těchto útocích přijdou, je přitom dost vysoká, zhruba čtvrt milionu korun,“ uvedla Monika Zahálková, výkonná ředitelka České bankovní asociace. Její slova potvrzuje i Lukáš Kintr, ředitel Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

„Žijeme v digitální době, která nám mnohé věci usnadňuje, ale také přináší mnohá rizika, a mezi ně patří i rostoucí počet různých kyberútoků. Detekujeme vysoké počty nejen podvodných telefonátů, ale i textových zpráv či e-mailů, a nelze očekávat, že by se jejich míra měla snižovat. Nejlepší obranou proti těmto pokusům nadále zůstává obecná osvěta,

tedy informovanost a poučenost veřejnosti, aby byli lidé schopni vishing a podobné snahy rozpoznat," upřesňuje Lukáš Kintr.

Přibývá také způsobů, jimiž se podvodníci snaží své oběti nachytat. Kromě tradičních podvodných e-mailů, SMS a již zmíněného vishingu se stále častěji setkáváme s podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze.

„Loňskou novinkou jsou také tzv. reverzní inzertní podvody, jejichž počet neustále roste. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou," objasnil brig. gen. Tomáš Kubík, náměstek policejního prezidenta pro kriminální policii.

#nePINdej! – celonárodní vzdělávací kampaň v oblasti kyberbezpečnosti

Kybernetická kriminalita také již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Česká bankovní asociace proto spouští rozsáhlou vzdělávací kampaň, která má upozornit na sílící nebezpečí podvodů na internetu. Pod názvem #nePINdej! představí nejčastější kybernetické útoky a formou hravého testu naučí, jak jim nenaletět. Kampaní chce ČBA oslovit širokou veřejnost – mladistvé od dvanácti let, dospělé i seniory.

Klíčovým prvkem kampaně #nePINdej! je interaktivní vzdělávací Kybertest, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. *„Název #nePINdej! funguje jako slovní hříčka a je vtipnou výzvou, aby si lidé dávali pozor na své citlivé údaje a chránili své peníze ve světě internetu. Zároveň bude na sociálních sítích i v dalších kanálech aktivizovat veřejnost k tomu, aby si ve speciálně vytvořené online aplikaci otestovala své schopnosti obstát před kyberútoky,"* říká Monika Zahálková, výkonná ředitelka České bankovní asociace.

Zdroj: Česká bankovní asociace

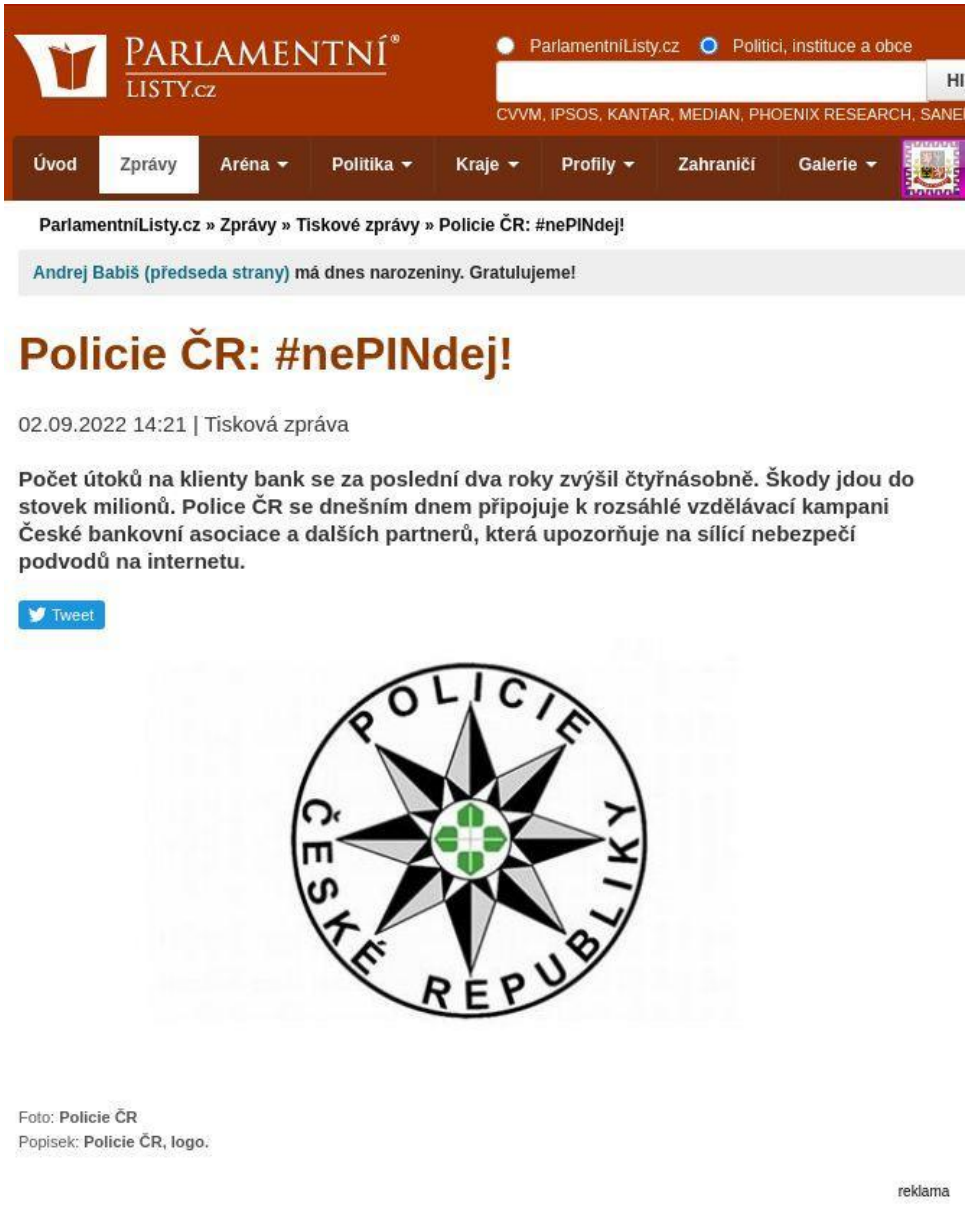
27. Policie ČR: #nePINdej!

Online ● parlamentnilisty.cz (Zprávy / Politika) ● 2. 9. 2022, 14:21

Vydavatel: **OUR MEDIA a.s. (cz-28876890)** ● Rubrika: **Tiskové zprávy**

Dosah: 166 191 ● GRP: 1.85 ● OTS: 0.02 ● AVE: 41735.40 Kč ● Interakcí: 11

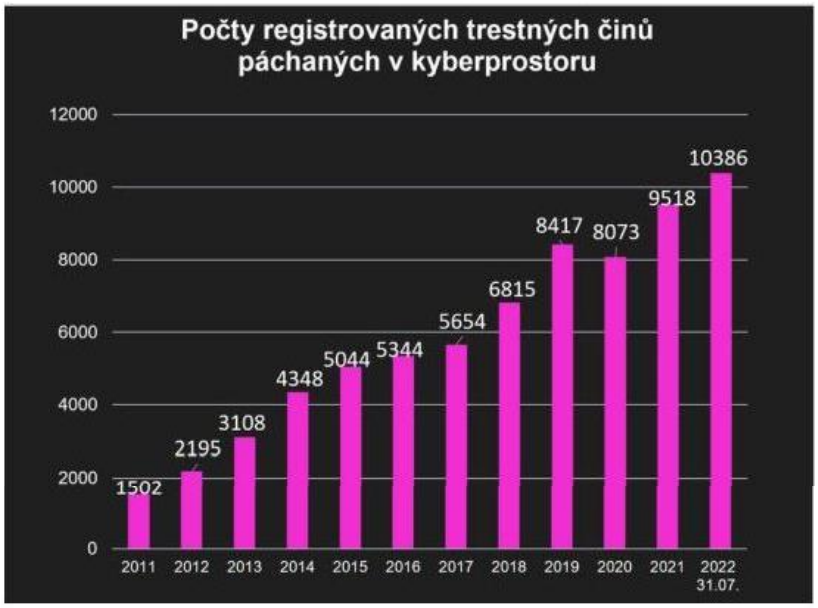
Odkaz: https://www.parlamentnilisty.cz/zpravy/tiskovezpravy/Policie-CR-nePINdej-713085



Jak vyplývá z dat České bankovní asociace získaných od jejích členských bank, na jednoho poškozeného klienta připadá průměrná škoda ve výši 161 500 korun. U vishingu, neboli případů podvodného navolávání, jsou částky až čtvrtmilionové.

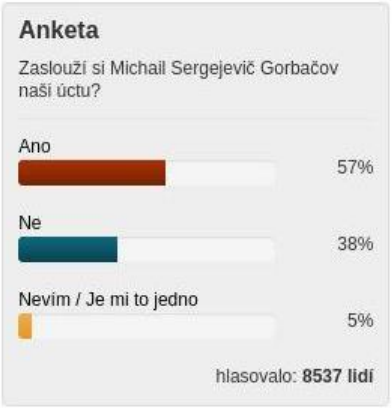
Klíčovým prvkem kampaně s názvem #nePINdej! (kreativní tvorba ze slov PIN nedej) je interaktivní vzdělávací www.kybertest.cz, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. Kybernetická kriminalita již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Kampaň proto cílí na širokou veřejnost počínaje dětmi a mladistvými přes dospělé až na seniory. „Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na nejstarší spoluobčany," vysvětluje Tomáš Trachta, člen představenstva společnosti itego, a.s., která pro ČBA kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně.

V kybertestu jsou simulovány podvodné SMS, zobrazovací okna k připojení k WIFI sítím, phishingové emaily, zvukové nahrávky podvodných telefonů a mnohé další, tak, aby si je každý uživatel moderních technologií mohl bezpečně vyzkoušet. Testové otázky byly připravovány odborníky na základě reálných případů, jimiž se podvodníci snaží své oběti nachytat. Kampaň #nePINdej! patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají. „Zároveň bude na sociálních sítích i v dalších kanálech aktivizovat veřejnost k tomu, aby si ve speciálně vytvořené online aplikaci otestovala své schopnosti obstát před kyberútoky," říká Monika Zahálková, výkonná ředitelka České bankovní asociace.



Pachatelé se při těchto útocích snaží překonávat zejména lidský faktor a pod nejrůznějšími legendami využívají nátlaku, strachu a časové tísně pro záchranu peněz nebo pro realizaci finanční transakce. Mezi nejčastější podvodné legendy patří:

Podvodné navolávání:
Pachatelé se vydávají například za bankéře, policisty, pracovníky technické podpory a snaží se z lidí pod vlivem strachu vylákat peníze, nebo vzdálený přístup do zařízení oběti, který následně zneužije.



Nabídka výhodných investic:
Přesvědčivá lákavá reklama a manipulativní jednání. Cílem pachatele je vylákat z oběti co možná nejvíce finančních prostředků a využívá k tomu přirozenou ziskuchtivost každého z nás.

Reverzní inzertní podvody:
Pachatel zareaguje na váš inzerát. Podstrčí vám fiktivní platební bránu, kde vyplníte citlivé bankovní údaje a místo peněz za inzerované zboží přicházíte o všechny úspory.

Podvody typu Nigerijské dopisy:
Princip, který funguje už více než 100 let. Pachatelé sázejí na kvantitu. Vždy se najde někdo, kdo se nechá nachytat na slibovanou cennou zásilku nebo domnělou pomoc. Často zde hraje velkou roli láska.

Klasické podvody typu phishing a smishing:
Stále dokonalejší a složitě rozpoznatelné podvodné emaily a SMS nabídky. Na první pohled již nenajdeme podezřelé znaky.

Kromě tradičních podvodných e-mailů, SMS a již zmíněného vishingu se stále častěji setkáváme s podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze. „Loňskou novinkou jsou také tzv. reverzní inzertní podvody, jejichž počet neustále roste. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou," objasnil brig. gen. Tomáš Kubík, náměstek policejního prezidenta pro kriminální policii.

Kyberkampaň #nePINdej! bude s ohledem na širokou cílovou skupinu probíhat napříč všemi médii – na internetu, v tisku, v České televizi, využita bude i tištěná reklama – formou letáků na pobočkách České pošty –, a pevné reklamní plochy ve vlacích a na nádražích Českých drah, ale i na bankomatech bank působících na českém trhu. Společnost O2 pak kampaň podpoří SMS

na bankomatech bank působících na českém trhu. Společnost O2 pak kampaň podpoří SMS zprávami s výzvou k účasti na testu. Ze sociálních sítí bude kromě standardních kanálů (Facebook, LinkedIn, Twitter, Instagram) nově využit i TikTok. Kampaň podpoří na svých profilech i influencer Martin „Mikýř" Mikyska.

Základní rady, jak nenaletět:

- Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.
- Vyzkoušej si kybertest (ZDE) a zjisti, kde máš mezery. Buď připraven.

Psali jsme:

Policie ČR: Zebra opět doprovází žáčky na jejich cestě do školy

Policie ČR: První předsednická konference Policie ČR hostí experty na nové technologie

Policie ČR: Vyhodnocení dopravně bezpečnostní akce

Policie ČR: Skončilo cvičení „MORAVA"

Líbil se Vám tento článek?

Nezávislost naší redakce můžete podpořit peněžitým darem v jakékoliv výši bankovním převodem na účet:

123 - 4175230287/0100

QR kód obsahuje údaje k platbě, výši částky si určete sami.

DĚKUJEME

Redakci PL můžete podpořit i zakoupením předplatného. Předplatitelům nezobrazujeme reklamy.

28. Cyberattacks on bank clients up fourfold in two years - CBA

Agenturní zpravodajství ● ČTK (ČTK) ● 2. 9. 2022, 16:51

Vydavatel: **Česká tisková kancelář (cz-47115068)** ● Autor: **hja, hel**

Odkaz: náhled

Prague, Sept 2 (CTK) - The number of cyberattacks on Czech bank clients has risen fourfold in the last two years, the damage per affected client amounting to Kc161,500 on average, according to data of the Czech Banking Association (CBA).
On Thursday, the CBA launched an extensive cybersecurity awareness campaign to last until December in cooperation with public bodies and big companies.
In the first seven months of 2022, there were twice as many cyberattacks on bank clients as in the whole of last year, vishing phone calls, one of the most insidious threats, having surged dramatically, the CBA's head Monika Zahalkova said at a press conference.
There were nearly 10,400 cyber crimes registered by the Czech police from January to the end of July 2022, compared to about 9,500 incidents recorded for the whole of last year, according to the Czech police statistics.
Although the Czech financial sector ranks among the most secure, according to the National Cyber and Information Security Agency (NUKIB), 81 percent of the country's financial institutions have reported a cyberattack attempt, with phishing, fraudulent e-mails and harmful codes being the most common.
Cyber frauds also multiplied on social media and second-hand e-commerce saw a new type of fraud last year where perpetrators attempt to inveigle sellers into giving them their payment card details.
The corner stone of the cyber awareness campaign is an interactive educational testing platform **Kybertest** which offers age group-tailored simulations of the most common fraudulent practices and teaches the public to recognise and avoid them, said Tomas Trachta of itego, an IT company that designed the tool.
The CBA is steering the campaign under the hashtag #nePINdej! along with the NUKIB, the Czech police, the Czech Post, the state-run rail carrier Ceske drahy, energy group CEZ, itego, Cisco, Thein Security, Mastercard and O2. The campaign's media partners include the public Czech Television, the Seznam Zpravy and Denik new sites and the Cinestar multiplex network.
hja/er/hel
Autor: hel, hja

29.#nePINdej!

Online ● policie.cz (Jiné) ● 2. 9. 2022, 17:30

Dosah: 20 667 ● GRP: 0.23 ● OTS: 0.00 ● AVE: 19996.45 Kč

Odkaz: https://www.policie.cz/clanek/uzemni-odbor-praha-venkov-vychod-zpravodajstvi-nepindej.aspx

ZPRAVODAJSTVÍ

Úvodní strana / Útvary Policie ČR / Krajská ředitelství policie / Středočeský kraj / Územr

Policie České republiky – KŘP Středočeského kraje

#nePINdej!

Praha venkov - VÝCHOD - Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně.

Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů. Police ČR se dnešním dnem připojuje k rozsáhlé vzdělávací kampani České bankovní asociace a dalších partnerů, která upozorňuje na sílící nebezpečí podvodů na internetu.

Jak vyplývá z dat České bankovní asociace získaných od jejích členských bank, na jednoho poškozeného klienta připadá průměrná škoda ve výši 161 500 korun. U vishingu, neboli případů podvodného navolávání, jsou částky až čtvrtmilionové.

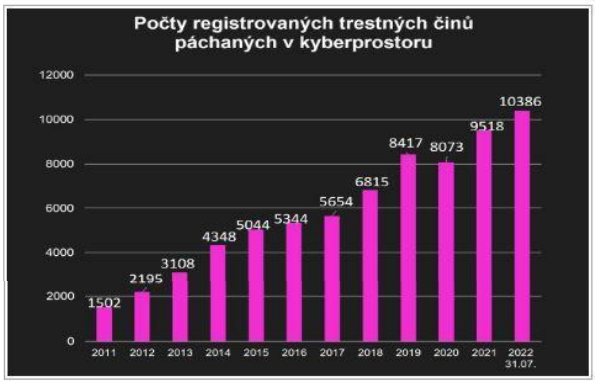
Klíčovým prvkem kampaně s názvem **#nePINdej!** (kreativní tvorba ze slov PIN nedej) je interaktivní vzdělávací **www.kybertest.cz**, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. Kybernetická kriminalita již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Kampaň proto cílí na širokou veřejnost počínaje dětmi a mladistvými přes dospělé až na seniory. *„Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na nejstarší spoluobčany,“* vysvětluje **Tomáš Trachta, člen představenstva společnosti itego, a.s.**, která pro ČBA kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně.

V kybertestu jsou simulovány podvodné SMS, zobrazovací okna k připojení k WIFI sítím, phishingové emaily, zvukové nahrávky podvodných telefonů a mnohé další, tak, aby si je každý uživatel moderních technologií mohl bezpečně vyzkoušet. Testové otázky byly připravovány odborníky na základě reálných případů, jimiž se podvodníci snaží své oběti nachytat. Kampaň #nePINdej! patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají. *„Zároveň bude na sociálních sítích i v dalších kanálech aktivizovat veřejnost k tomu, aby si ve speciálně vytvořené online aplikaci otestovala své schopnosti obstát před kyberútoky,“* říká **Monika Zahálková, výkonná ředitelka České bankovní asociace**.

Pachatelé se při těchto útocích snaží překonávat zejména lidský faktor a pod nejrůznějšími legendami využívají nátlaku, strachu a časové tísně pro záchranu peněz nebo pro realizaci finanční transakce. Mezi nejčastější podvodné legendy patří:

Podvodné navolávání:

- Pachatelé se vydávají například za bankéře, policisty, pracovníky technické podpory a snaží se z lidí pod vlivem strachu vylákat peníze, nebo vzdálený přístup do zařízení oběti, který následně zneužije.



Nabídka výhodných investic: *Počty registrovaných TČ páchaných v kyberprostoru.jpg*

- Přesvědčivá lákavá reklama a manipulativní jednání. Cílem pachatele je vylákat z oběti co možná nejvíce finančních prostředků a využívá k tomu přirozenou získuchtivost každého z nás.

Reverzní inzertní podvody:

- Pachatel zareaguje na váš inzerát. Podstrčí vám fiktivní platební bránu, kde vyplníte citlivé bankovní údaje a místo peněz za inzerované zboží přicházíte o všechny úspory.

Podvody typu Nigerijské dopisy:

- Princip, který funguje už více jak 100 let. Pachatelé sázejí na kvantitu. Vždy se najde někdo, kdo se nechá nachytat na slibovanou cennou zásilku nebo domnělou pomoc. Často zde hraje velkou roli láska.

Klasické podvody typu phishing a smishing:

- Stále dokonalejší a složitě rozpoznatelné podvodné emaily a SMS nabídky. Na první pohled již nenajdeme podezřelé znaky.

Kromě tradičních podvodných e-mailů, SMS a již zmíněného vishingu se stále častěji setkáváme s podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze. *„Loňskou novinkou jsou také tzv. reverzní inzertní podvody, jejichž počet neustále roste. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou,"* objasnil **brig. gen. Tomáš Kubík, náměstek policejního prezidenta pro kriminální policii**.

Kyberkampaň #nePINdej! bude s ohledem na širokou cílovou skupinu probíhat napříč všemi médii – na internetu, v tisku, v České televizi, využita bude i tištěná reklama – formou letáků na pobočkách České pošty –, a pevné reklamní plochy ve vlacích a na nádražích Českých drah, ale i na bankomatech bank působících na českém trhu. Společnost O2 pak kampaň podpoří SMS zprávami s výzvou k účasti na testu. Ze sociálních sítí bude kromě standardních kanálů (Facebook, LinkedIn, Twitter, Instagram) nově využit i TikTok. Kampaň podpoří na svých profilech i influencer Martin „Mikýř" Mikyska.

Základní rady, jak nenaletět

- Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.
- Vyzkoušej si **www.kybertest.cz** a zjisti, kde máš mezery. Buď připraven.

plk. Zuzana Pidrmnaová
vedoucí oddělení prevence

Související dokumenty

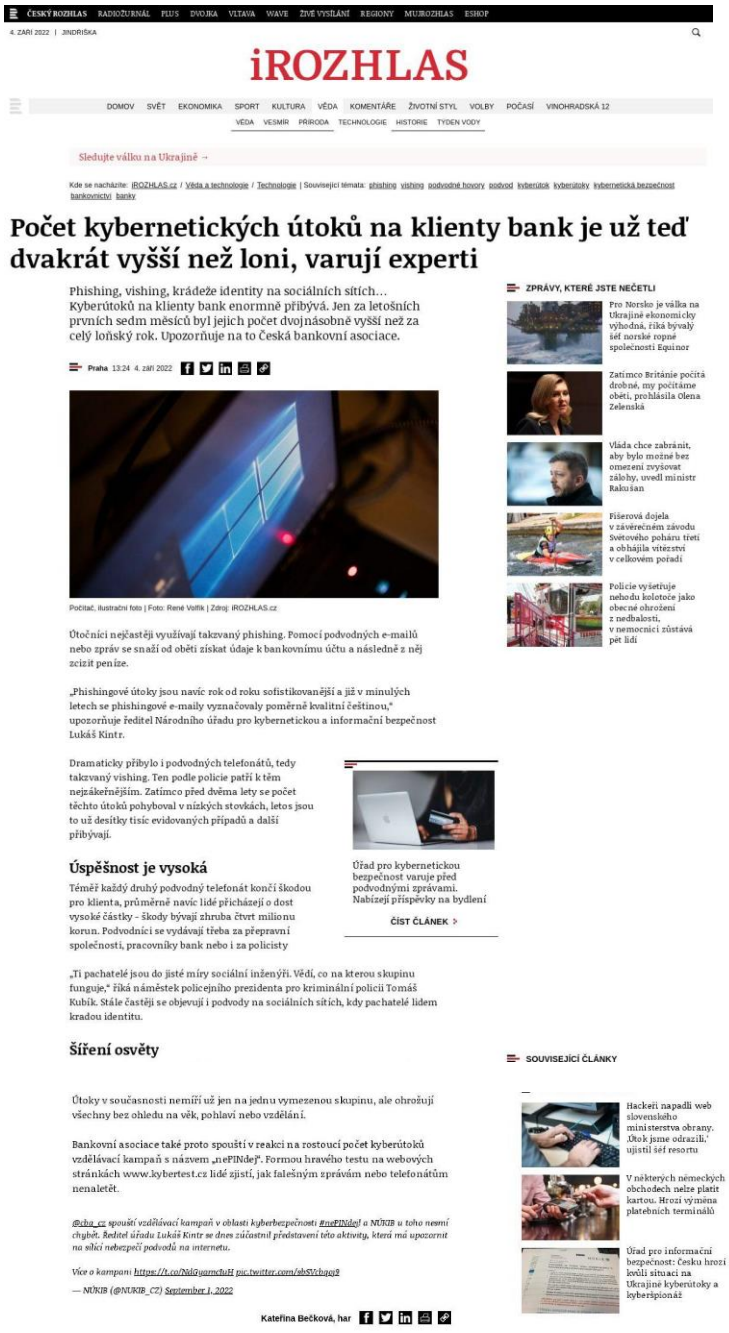
30. Počet kybernetických útoků na klienty bank je už teď dvakrát vyšší než loni, varují experti

Online ● irozhlas.cz (Zprávy / Politika) ● 4. 9. 2022, 13:24

Vydavatel: **ČESKÝ ROZHLAS (cz-45245053)** ● Autor: **Kateřina Bečková, Miroslav Harant**

Dosah: 146 626 ● GRP: 1.63 ● OTS: 0.02 ● AVE: 38505.80 Kč ● Interakcí: 26

Odkaz: https://www.irozhlas.cz/veda-technologie/technologie/kyberutoky-phishing-podvodne-telefonaty-vyssi-pocet_2209041324_har



ČESKÝ ROZHLAS RADIOŽURNÁL PLUS DVOJKA VLTAVA WAVE ŽIVÉ VYSÍLÁNÍ REGIONY MUJROZHLAS ESHOP

4. ZÁŘÍ 2022 | JINDŘIŠKA

iROZHLAS

DOMOV SVĚT EKONOMIKA SPORT KULTURA VĚDA KOMENTÁŘE ŽIVOTNÍ STYL VOLBY POČASÍ VINOHRADSKÁ 12

VĚDA VESMÍR PŘÍRODA TECHNOLOGIE HISTORIE TÝDEN VODY

Sledujte válku na Ukrajině →

Kde se nacházíte: iROZHLAS.cz / Věda a technologie / Technologie | Související témata: phishing vishing podvodné hovory podvod kyberútok kyberútoky kybernetická bezpečnost bankovnictví banky

Počet kybernetických útoků na klienty bank je už teď dvakrát vyšší než loni, varují experti

Phishing, vishing, krádeže identity na sociálních sítích… Kyberútoků na klienty bank enormně přibývá. Jen za letošních prvních sedm měsíců byl jejich počet dvojnásobně vyšší než za celý loňský rok. Upozorňuje na to Česká bankovní asociace.

Praha 13:24 4. září 2022

Počítač, ilustrační foto | Foto: René Volfík | Zdroj: iROZHLAS.cz

Útočníci nejčastěji využívají takzvaný phishing. Pomocí podvodných e-mailů nebo zpráv se snaží od oběti získat údaje k bankovnímu účtu a následně z něj zcizit peníze.

„Phishingové útoky jsou navíc rok od roku sofistikovanější a již v minulých letech se phishingové e-maily vyznačovaly poměrně kvalitní češtinou," upozorňuje ředitel Národního úřadu pro kybernetickou a informační bezpečnost Lukáš Kintr.

Dramaticky přibylo i podvodných telefonátů, tedy takzvaný vishing. Ten podle policie patří k těm nejzákeřnějším. Zatímco před dvěma lety se počet těchto útoků pohyboval v nízkých stovkách, letos jsou to už desítky tisíc evidovaných případů a další přibývají.

Úřad pro kybernetickou bezpečnost varuje před podvodnými zprávami. Nabízejí příspěvky na bydlení

ČÍST ČLÁNEK >

Úspěšnost je vysoká

Téměř každý druhý podvodný telefonát končí škodou pro klienta, průměrně navíc lidé přicházejí o dost vysoké částky - škody bývají zhruba čtvrt milionu korun. Podvodníci se vydávají třeba za přepravní společnosti, pracovníky bank nebo i za policisty

„Ti pachatelé jsou do jisté míry sociální inženýři. Vědí, co na kterou skupinu funguje," říká náměstek policejního prezidenta pro kriminální policii Tomáš Kubík. Stále častěji se objevují i podvody na sociálních sítích, kdy pachatelé lidem kradou identitu.

Šíření osvěty

Útoky v současnosti nemíří už jen na jednu vymezenou skupinu, ale ohrožují všechny bez ohledu na věk, pohlaví nebo vzdělání.

Bankovní asociace také proto spouští v reakci na rostoucí počet kyberútoků vzdělávací kampaň s názvem „nePINdej". Formou hravého testu na webových stránkách www.kybertest.cz lidé zjistí, jak falešným zprávám nebo telefonátům nenalétět.

@cba_cz spouští vzdělávací kampaň v oblasti kyberbezpečnosti #nePINdej a NÚKIB u toho nesmí chybět. Ředitel úřadu Lukáš Kintr se dnes zúčastnil představení této aktivity, která má upozornit na sílící nebezpečí podvodů na internetu.

Více o kampani https://t.co/NdGgarnctuH pic.twitter.com/ebSYcbqoj8

— NÚKIB (@NUKIB_CZ) September 1, 2022

Kateřina Bečková, har

ZPRÁVY, KTERÉ JSTE NEČETLI

Pro Norsko je válka na Ukrajině ekonomicky výhodná, říká bývalý šéf norské ropné společnosti Equinor

Zatímco Británie počítá drobné, my počítáme oběti, prohlásila Olena Zelenská

Vláda chce zabránit, aby bylo možné bez omezení zvyšovat zálohy, uvedl ministr Rakušan

Píšerová dojela v závěrečném závodu světového poháru třetí a obhájila vítězství v celkovém pořadí

Policie vyšetřuje nehodu kolotoče jako obecné ohrožení z nedbalosti, v nemocnici zůstává pět lidí

SOUVISEJÍCÍ ČLÁNKY

Hackeři napadli web slovenského ministerstva obrany. „Rok jsme odrazili," ujistil šéf resortu

V některých německých obchodech nelze platit kartou. Hrozí výměna platebních terminálů

Úřad pro informační bezpečnost: Česku hrozí krvavá situace na Ukrajině kyberútoky a kyberšpionáž

31. Kybertest ukáže, jak nenaletět

Tisk ● Právo - Karlovarsko; str. 12 (Zprávy / Politika) ● 5. 9. 2022

Vydavatel: **BORGIS a.s. (cz-00564893)** ● Autor: **gin**

Dosah: 140 000 ● GRP: 1.56 ● OTS: 0.02 ● AVE: 25302.18 Kč

Odkaz: náhled

STRANA 12 TRHY & EKONOMIKA PONDĚLÍ 5. ZÁŘÍ 2022 ◇ PRÁVO

Nových dálnic bude i příští rok jen 25 km

Tomáš Volf

Řidiči by se měli ještě do konce letošního roku projet po 25 kilometrech nových dálnic a podobný nevelký přírůstek lze čekat v roce příštím, i když premiér Petr Fiala (ODS) nedávno po rok 2023 optimisticky slíbil více, 40 kilometrů.

Jedná se o projekty, které připravila ještě minulá vláda Andreje Babiše (ANO), což vládě při čtvrtečním proslovu před hlasováním o nedůvěře Fialově kabinetu připomněl samotný šéf ANO.

„To mě strašně pobavilo, když pan premiér navštívil ministerstvo dopravy a zjistil, že je ve výstavbě 240 kilometrů. Ano, pane premiére, to je naše dílo," prohlásil Babiš. „Vy nikdy neřeknete, co bylo za nás," postěžoval si.

Ministr dopravy Martin Kupka (ODS) nicméně už v rozhovoru pro Právo po nástupu do funkce loni v prosinci připustil, že projekty dopravního stavitelství jdou nad rámec jednoho i více volebních období.

Obchvat uleví Frýdku-Místku

Loni bylo nových úseků dálnic víc, povedlo se otevřít 47 kilometrů dálnic. Ale ne vždy tomu tak v minulosti bylo, i za ANO. Jeho ministr dopravy Dan Ťok čelil v roce 2018 silné kritice za to, že se podařilo zprovoznit pouhé čtyři kilometry, ačkoliv mezitím probíhala ještě zmíněná modernizace D1, o níž rozhodla před lety vláda Petra Nečase (ODS).

> To je naše dílo, pane premiére. Nikdy neřeknete, co bylo za nás
>
> *Andrej Babiš (ANO)*

Nejnověji se minulý pátek motoristům otevřela 6,5 kilometru dlouhá část obchvatu Frýdku-Místku na D48 s připojením na D56. Podle Ředitelství silnic a dálnic ČR (ŘSD) jde o první letos zprovozněnou dálniční stavbu, i když na její část v jednom směru pustili řidiče již na konci června.

Poslední čtyři kilometry obchvatu, na který místní čekají desítky let, by se měly otevřít v částečném provozu do konce roku. Stavbu zkomplikoval i sesuv půdy a za zdržením stály i stížnosti ekologického sdružení Děti Země, které napadalo vydané stavební povolení.

Dokončení staveb na dálnicích v letošním a příštím roce

„Jednoznačně přínosem je odvedení tranzitní dopravy z Frýdku-Místku, v tuto chvíli zejména v severojižním směru, ve směru od západu, od Olomouce, na jih do Beskyd," řekl generální ředitel ŘSD Radek Mátl.

Letos také ŘSD plánuje otevřít skoro 15 kilometrů dlouhý úsek D35 z Časů do Ostrova, navíže na loni otevřenou část Opatovice – Časy. Celá D35 ale má být hotová do roku 2028, kdy bude možné dojet z Prahy až do Olomouce severní trasou.

Předseda vlády Fiala předminulý týden po bilančním sečtání s ministrem Kupkou prohlásil, že více se postaví příští rok. Slíbil přes 40 kilometrů dálnic. Premiéra ale ještě týž den korigoval Kupka. „Pro ten příští rok se to zřejmě ještě bude muset snížit," prohlásil. Jak Právu upřesnil ředitel ŘSD Mátl, zprovoznění 40 km nových dálnic pro rok 2023 je opravdu optimistický odhad. „Ten předpokládá urychlení zprovoznění druhé části stavby D48 Bělotín – Rybí, konkrétně část Palačov – Rybí, kde řešíme problematiku potenciálního sesuvu. A dál stavby D55 Babice – Staré Město – Moravský Písek, u kterých je termín zprovoznění plánován na jaro 2024," popsal.

Realistický odhad proto směřuje k zhruba 25 km. „Skutečný boom nastane v roce 2024, kdy by mělo být zprovozněno až 100 km nových dálnic," řekl už dříve Právu Mátl.

Prodloužení D3 a obchvat Loun

Pro příští rok je v plánu otevřít ještě šestikilometrový obchvat Loun na D7 a cestu na jih urychlit prodloužení D3 Hodějovice – Třeboňin, kde půjde o 12,6 kilometru. Řidiči musí počítat s tím, že nové úseky se obvykle otevírají až na konci roku, často v prosinci.

Kupka po uvedení do funkce loni v prosinci slíbil, že jeho cílem je během čtyřletého volebního období otevřít 200 kilometrů nových dálnic. Zda se mu cíl podaří splnit, by měl do velké míry naznačit rok 2024, kdy by mělo být mimo jiné dokončeno 32 kilometrů nové D4, které staví konsorcium Via Salis a zhotovitelem je DIVIA stavební ze skupiny Eurovia. Jedná se o první PPP projekt, tedy o spolupráci státu se soukromníkem, který ovšem také připravila ještě Babišova vláda.

Zadej kartu, zbohatneš jako Musk, lákají podvodné weby

Jindřich Ginter

Český internet zaplavily v poslední době v nebývalé míře podvodné weby, které často působí až hlaznivě. Tváří se seriózně, jsou v češtině, ale přitom nejde o nic jiného než o snahu lidi zmást a vytáhnout z nich podlouhé peníze. Nebo jde o obchody, kde se zákazník s reklamací nedovolá.

Jen za poslední dva měsíce Česká obchodní inspekce (ČOI) detekovala přes čtyři desítky zcela anonymních obchodních či výslovně podvodných stránek.

„V podstatě každý druhý den inspektoři zachytí jeden až dva takové případy a zveřejní je v přehledu rizikových e-shopů na stránkách ČOI. Z výčtu jasně vyplývá, že podvodníci už pomalu nevědí, čím by ještě lidi na sítích zaujali, a tak některé stránky působí už jako ze špatné komedie.

Tak například web „illuminatisofficial" zneužívá loga zpravodajských portálů a snaží se vytvořit dojem, že přináší novou zajímavou zprávu o zázračném zbohatnutí zakladatele Tesly a SpaceX a nejbohatšího člověka planety Elona Muska.

V dalším kroku už ale stránka po uživateli chce, aby zadal své osobní údaje i údaje o platební kartě, což má vést údajně k obdobnému zbohatnutí jako v Muskově případě.

„Systém na základě lživých informací žádá velmi citlivá data. Jako provozovatel webu není uveden nikdo," varovala ČOI.

Na podobném principu fungují podvodníci i na webu zpravy-24.com. „Stránka ale není skutečným zpravodajským webem, nýbrž nabídkou až zázračných přípravků pro lidské zdraví. Vytváří pocit, že jde o seriózní články o neznámých přípravcích, které je pak možné zakoupit. Prodejce je však zcela anonymní," uvedla inspekce.

Nebo trojice webů golden-dood.shop, veryuseful.ml, med-group.club, na něž odkazuje reklama na Facebooku, zneužívá jméno známého českého lékaře Jana Pirka. „Ten se od nich distancoval. Stránky jsou anonymní a nabízejí pod smyšleným převratným vynálezem českého lékaře neznámý přípravek," varovala ČOI.

DHL Ulánbátar

Opravdu vypečená je podvodná stránka https://archive.ulaanbaatar.mn/curl/m4/. Předstírá, že jde o platební stránku logistické společnosti DHL. V pozadí je zobrazeno letadlo v barvách DHL a v popředí formulář na vyplnění údajů z platební karty. Koho nezarazí bizarní odkaz na hlavní město Mongolska Ulánbátar a své údaje poskytne, tomu podvodníci vezmou peníze z účtu.

Líbivě působí web problemyshoklama.cz obsahující velké fotografie mladých lidí.

Nabízí drobnosti do domácnosti, třeba pletací jehlice s bambusovou rukojetí, gelové propisovačky. Popis zboží je ale neobrabaný, strojový a ani zde není uveden žádný provozovatel. „Spotřebitel neví, s kým uzavírá smlouvu," upozornila inspekce.

Některé e-shopy z černé listiny ČOI jsou už dnes nefunkční, jiné vesele jedou dál, jako stránky happyshop-cz.com. Nabízejí „vše pro váš domov a zábavu pro celou rodinu". Třeba keramickou pánev nebo LED osvětlení. Provozovatel je opět neznámý, v kontaktech je uveden jen e-mail a formulář.

„Tento obchod může u spotřebitelů vzbuzovat dojem, že je provozován subjektem se sídlem v České republice nebo Evropské unii," podotkla ČOI. Podle ní je však provozován z Číny, takže možnost uplatňovat svá práva mají spotřebitelé významně ztíženou.

NortonLifeLock může převzít Avast

Britský antimonopolní úřad (CMA) definitivně schválil převzetí české antivirové společnosti Avast americkou softwarovou firmou NortonLifeLock za 8,6 miliardy USD (211,2 miliardy Kč). Trh s bezpečnostním softwarem zůstane podle úřadu konkurenční i po spojení obou firem. Úřad tak potvrdil své předběžné rozhodnutí z minulého měsíce. **(ČTK)**

Přibylo nejvíce živností za pět let

Od začátku roku do července přibylo v ČR celkem 14 883 živnostníků, což odpovídá nejvyššímu čistému přírůstku podnikatelů během prvních sedmi měsíců od roku 2017. Podnikat v tomto období začalo 43 964 fyzických osob – opět nejvíce od roku 2017 – a naopak svou živnost ukončilo 29 081 podnikatelů. Vyplývá to z analýzy společností ČRIF – Czech Credit Bureau.

Méně leasingu

Zatímco v prvním čtvrtletí letošního roku zaznamenala Česká leasingová a finanční asociace (ČLFA) oživení zájmu o financování nových osobních automobilů (+2,7 %), ve druhém čtvrtletí došlo k meziročnímu propadu o 11,7 %. Za prvních šest měsíců tak meziročně poklesl počet financovaných nových osobních vozů o dva tisíce na 24 907. **(gin)**

Apple už v USA porazil Android

Technologický obr Apple ve Spojených státech předběhl operační systém Android od konkurenční společnosti Google. Na tamním trhu už měly v červnu chytré telefony Apple nadpoloviční podíl, což je historicky nejvíce od představení první generace telefonu iPhone v roce 2007.

Zbylý podíl si mezi sebou dělí asi 150 značek s Androidem, největší podíl mezi nimi mají telefony jihokorejského Samsungu a čínského Lenova. Čísla zveřejnila společnost Counterpoint. **(pro)**

Kybertest ukáže, jak nenaletět

Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů a na jednoho poškozeného činí v průměru 161 500 Kč. Vyplynulo to z dat České bankovní asociace (ČBA). Ta proto spustí rozsáhlou vzdělávací kampaň #nePINdej!

Klíčovým prvkem kampaně je interaktivní vzdělávací Kybertest na stránce www.kybertest.cz, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět.

„Letos za prvních sedm měsíců byl počet útoků dvojnásobně vyšší než za celý loňský rok," sdělila výkonná ředitelka ČBA Monika Zahálková.

Dramaticky narostly podvodné telefonáty, tzv. vishing. Před dvěma lety se jejich počet pohyboval ve stovkách, letos jsou to desítky tisíc. Průměrné částka, o kterou klienti při těchto útocích přijdou, je čtvrt milionu korun. **(gin)**

Americký soud zamítl žalobu proti Vítkově CPI

Americký odvolací soud zamítl žalobu proti realitní skupině CPI Property Group Radovana Vítka.

Tu na společnost podal v dubnu 2019 hedgeový fond Kingstown a další strany včetně firem některých manažerů Mostecké uhelné společnosti (MUS) Marka Čmejly a Jiřího Diviše.

Spor se týkal převzetí firmy Orco Property Group, kterým údajně Vítek připravil žalobce o více než miliardu dolarů (přes 24 miliard korun). CPI vinu dlouhodobě odmítala. „CPIPG od prvního dne tvrdila, že žaloba nemá opodstatnění," řekl generální ředitel Martin Němeček. „Jsme potěšení dnešním rozhodnutím. Spravedlnosti bylo učiněno zadost," dodal.

Jádrem sporu je podle dřívějších informací Deníku N ovládnutí Orco Property Group Radovanem Vítkem. Podle žaloby poté, co část podílu ve skupině získal Kingstown Capital Management, Vítek vymyslel plán, jak skupinu skrytě ovládnout.

Podle žaloby poté vytunelovával její nejhodnotnější části, přičemž nemovitosti prodával pod cenou třetím subjektům, které podle žaloby skrytě ovládal. Žalobci požadovali po Vítkovi kolem 70 miliard korun, což byl trojnásobek údajné škody. **(ČTK, zr)**

Burza v Praze klesla na roční minimum

Akcie na pražské burze během uplynulého týdne opět oslabily. Index PX klesl o 3,1 procenta a dostal se nejníže od loňského července.

Výrazně oslabovaly akcie ČEZ, Komerční banky a Monety Money Bank. Erste Bank naopak posílila a protrhla tak šňůru tří týdnů poklesu. Největší růst zaznamenaly akcie zbrojovky Colt CZ Group.

Akcie ČEZ za týden přišly o šest procent a prodávaly se za 948,50 koruny. „Pravděpodobně je to dáno hrozbou speciální daně," komentoval ekonom KB Bohumil Trampota.

Mimořádnou daň zvažuje vláda pro sektory energetických firem, bank či rafinerií.

Erste začátkem týdne prohloubila téměř dvouletá minima, celkově ale během týdne její akcie posilovaly. Vzrostly o 1,47 procenta na 550,60 koruny. Naopak Komerční banka oslabila o 4,88 procenta na 574,50 koruny a Moneta ztratila 6,08 procenta na 74,20 koruny. Nejvýrazněji oslabovaly akcie firmy solární společnosti Photon Energy, a to hlavně kvůli výraznému páteřnímu propadu, kdy ztratily skoro 13 procent. Celkem během týdne poklesly o 22,74 procenta na 63,20 koruny.

Česká měna v závěru týdne nepatrně oslabila vůči euru na 24,54 Kč/EUR. K dolaru naopak zpevnila o zhruba 20 haléřů na 24,47 Kč/USD. **(tov, ČTK)**

Kurzy ČNB od 2. 9.

Země	Množství	Kód	Kurz
Austrálie	1	AUD	16,693
Čína	1	CNY	3,548
Dánsko	1	DKK	3,292
EMU	1	EUR	24,485
Chorvatsko	1	HRK	3,255
Japonsko	100	JPY	17,449
Kanada	1	CAD	18,654
Maďarsko	100	HUF	6,149
Polsko	1	PLN	5,203
Švýcarsko	1	CHF	24,889
Turecko	1	TRY	1,345
USA	1	USD	24,512
V. Británie	1	GBP	28,315

32. Michal Špaček: Před připojováním na veřejné Wi-Fi sítě už nevaruju

Online ● lupa.cz (IT / Technologie) ● 5. 9. 2022, 6:30

Vydavatel: **Internet Info, s.r.o. (cz-25648071)** ● Autor: **David Slížek**

Dosah: 27 681 ● GRP: 0.31 ● OTS: 0.00 ● AVE: 22778.02 Kč ● Interakcí: 1

Odkaz: https://www.lupa.cz/clanky/michal-spacek-pred-pripojovanim-na-verejne-wi-fi-site-uz-nevaruju/

vytváření hesel nejdůležitější. Jak silná hesla vytvářet? Jak dnes postupují útočníci? A kdy se dočkáme budoucnosti bez hesel? Uvnitř: PODCAST.

Ani používání vícefaktorového ověřování není stoprocentní zárukou, že vám odhodlaný útočník nenaboural účet. Je potřeba vybrat si tu správnou metodu, která je jen těžko napadnutelná, říká bezpečnostní expert Michal Špaček.

Stále podle něj platí, že dobrou metodou pro vytváření hesel je složení věty z několika náhodně vybraných slov. Je ale potřeba, aby jejich výběr byl skutečně náhodný a aby nešlo o sousloví, které se někde používá. „Jednou se mi podařilo cracknout třeba heslo ‚Kobyla má malý bok‘," ilustruje Špaček, jak není bezpečné používat jako heslo třeba známý palindrom. „Prostě lidi často slyší, že mají používat větu, tak použijí nějakou větu," krčí rameny.

Přečtěte si také:

Proč se (ne)přihlašovat přes Seznam.cz

„Před připojováním na veřejné Wi-Fi už nevaruju, protože většina stránek používá šifrované spojení přes HTTPS," říká také. „Kdybych se na veřejné Wi-Fi přihlásil do internetového bankovnictví přes aplikaci své banky a někdo mi odchytil moje přihlašovací údaje, bylo by to fakt špatné – ale ne kvůli Wi-Fi, ale protože by ta aplikace byla špatně napsaná," dodává.

Jak mohou útočníci vícefaktorové ověřování prolomit? Jak poznáte špatný článek o silných heslech? A co přinese plánované zavádění přihlašování bez hesel, přes tzv. passkeys? Část rozhovoru najdete níže v textové podobě, celý si jej můžete poslechnout jako podcast:

Michale, naposledy jsi pro Lupu psal článek o vytváření silných hesel v roce 2019. Změnilo se za ty tři roky něco zásadního v oblasti bezpečnosti a v oblasti toho, jak teda vytvářet silná hesla a jak si je potom zapamatovat?

Nezměnilo a tím tenhle rozhovor můžeme ukončit (smích).

Díky moc. Tak to byl Michal Špaček. Přečtěte si článek z roku 2019 a chovejte se podle něj (smích).

Nezměnilo se nic zásadního. A to je i důvod, proč jsem nic dalšího nenapsal. Takže tady mám krásnou výmluvu, že nemusím nic psát, protože se nic nezměnilo (smích). V podstatě pořád jsou důležitá unikátní hesla. Trošku začíná být možná důležitější dvoufaktorové ověřování (2FA), a to ještě to správné. Existuje dvoufaktorové ověřování přes SMS, přes aplikaci, přes takový ten „čudl", který se strká do USB, a začíná být důležitější, který si vybrat.

Protože třeba z SMS pořád lze phishingem ověřovací kód získat. Phishingová stránka požádá o jméno a heslo a za chvilku požádá, aby jí lidi přepsali i kód z SMS. Phishingem tedy může být možné váš kód získat, ale třeba z toho USB tokenu ne, protože tam se vlastně nic nepřepisuje.

Takže hardwarové tokeny jsou pořád nejlepším způsobem zabezpečení, o něco málo bezpečnější jsou mobilní aplikace, které mi napíšou upozornění, že musím něco potvrdit, a zasílání jednorázového hesla v SMS nebo e-mailem je méně bezpečné. Je to pořád tak?

Je to přesně tak. Samozřejmě e-mail a SMS dneska používá každý, takže je tento způsob pro uživatele levný a tím je víc použitelný. USB tokeny jsou mnohem lepší, bezpečnější, nedají se „phishnout", ale zase je tam nějaká investice. Teď jde o to, jestli tu investici chce udělat soukromá osoba. Rozhodně bych ji doporučoval firmám, protože phishingy na firmy jsou pro útočníky tučnější a šťavnatější a jde o víc peněz – a ne jenom peníze, občas třeba i o nějaká firemní tajemství a podobně. Takže firmám bych doporučoval do tokenů zainvestovat a nasadit je mezi všechny zaměstnance.

V médiích se často píše, že musíte mít 2FA a budete mít účet totálně zabezpečený. No, nemusí to být úplně pravda. Nedávno jsem četl o útoku, kdy uživatel používal mobilní aplikaci, kde se ověřuje tím, že jenom klikne na to, že

to je on. A útočníci mu začali posílat tu výzvu jednu za druhou. A co ten uživatel v takovém případě udělá? Poprvé klikne, že to není on. Za vteřinu zase ne a za další vteřinu znovu. Ale když mu to takhle chodí 10 minut, tak si řekne, že už toho má plné zuby a že je v té aplikaci asi nějaká chyba. Tak klikne na ano, to jsem já, a ono to přestane. A tím útočníci získali potvrzení, stačilo zahltit uživatele věcmi, které zrovna v tu chvíli nechtěl řešit.

To je zajímavý způsob, jak vícenásobné ověřování jakoby ne obejít, ale využít jeho vlastností pro záměry útočníků. Ukazuje se, že samozřejmě není dokonalé a je potřeba s tím počítat.

Takže když mě začne ta aplikace takto spamovat požadavky na potvrzení přihlášení, může to být signál, že se děje něco špatně?

Ano, může. Samozřejmě to taky může být nějaký bug v aplikaci, ale spíš asi ne.

Jak má dneska vypadat dobré silné heslo? Už před několika lety se doporučovalo, že má mít třeba minimálně čtrnáct znaků. Nedávno jsem někde na sociálních sítích viděl tabulku, kde počítali, jak dlouho trvá hrubou silou hesla prolomit v závislosti na jejich délce. Lámalo se to myslím až někde kolem dvaceti znaků. Kratší hesla byla relativně jednoduše prolomitelná. Je to tak? Je nějaký limit, jak dlouhá by hesla měla být, aby byla pořád relativně bezpečná?

Já ti na to odpovím malinko oklikou. Tu tabulku jsem samozřejmě viděl taky, běhá po síti v různých modifikacích, ale není u ní napsaný žádný kontext: třeba jak jsou ta hesla ukládaná nebo do jakého systému by se útočník snažil přihlásit. A bez kontextu ta tabulka obsahuje v podstatě náhodná čísla, protože kontext je opravdu důležitý. Kdyby bylo třeba heslo v čitelné podobě, tak se vůbec není potřeba pokoušet ho nijak lámat. Pokud bude uložené správným pomalým tzv. password hashem, tak by ta tabulka zase vypadala úplně jinak – byla by jiná pro každý algoritmus. Takže ta tabulka bez kontextu nedává moc smysl. Snažil jsem se dohledat, kde vlastně vznikla. Zjistil jsem, že je asi 10 let stará a platila pro přihlašování do počítačů s Windows.

Můžeme dát čtenářům odkaz na tabulku, která má přímo vypsané jednotlivé algoritmy, a ta je o něco lepší tam a je v ní vidět, kde se to láme.

A teď se vrátím k tomu, jak vlastně má vypadat silné heslo. Mám pravidlo, kterému pracovně říkám Špačkovo pravidlo špatných článků o heslech. To pravidlo zní tak, že pokud v nadpisu článku je heslo v jednotném čísle, čili „jak udělat silné heslo“, tak ten článek bude vždycky špatný. Pokud je v nadpisu „jak mít silná hesla“ – tedy v množném čísle – tak ten článek bude dobrý. A bohužel mi to takhle vychází. Vždycky, když čtu článek, kde je napsáno „jak mít silné heslo“, tak tam mluví o tom, jak má mít speciální znaky, kolik má mít znaků, jak často se má měnit, že tam musí být malé a velké písmeno, číslice, speciální znaky, hieroglyfy a názvy dinosaura (smích). Ale ten článek vůbec nemluví

o tom, co je nejdůležitější: že se to heslo nesmí používat na jiném místě.

Pokud ale článek v nadpisu má „jak mít silná hesla“, tak je velká šance, že hned na začátku řekne, že hesla musíte mít hlavně unikátní. A ten zbytek není tak důležitý jako to mít každé heslo jiné. Nechci úplně nabádat čtenáře, aby měli tříznaková hesla, to rozhodně ne. Ale osmiznaková nebo desetiznaková hesla mohou být v pohodě, pokud nejsou použitá vůbec nikde jinde.

S tím, jak stoupá výkon počítačů, opravdu nehrozí, že když heslo má třeba těch 8 znaků, tak že potom jde tou výpočetní sílu prolomit?

Pokud vezmeme online útoky, čili když by útočník nebo jeho nějaký robot, program, opravdu zadával hesla do formulářů na webu a snažil se třeba přihlásit na Lupu, Seznam nebo na Google, tak tam je to hodně pomalé a prolomit i to osmiznakové heslo by trvalo fakt dlouho a tyhle tzv. online útoky se běžně nedělají.

Offline útok pak spočívá v tom, že útočník někde sežene databázi nějak uložených hesel a snaží se z ní ta hlesla vylámat. Jenže ve chvíli, kdy už má tu databázi, existuje velká šance, že měl přístup hlouběji do systému a k údajům, která běžně hesla v aplikaci chrání, se stejně dostal.

Útočníci většinou ta hesla ukradnou z nějakých e-shopů a podobně, kde není uloženo nic zajímavého, a pak se s nimi snaží přihlásit třeba do e-mailu, kde už jsou uloženy zajímavější data (například kontakty), do banky a tak podobně. Takže i kdyby mi prolomili heslo na jakýkoliv e-shop, tak by mi to až tak nevadilo. Důležité je, že je unikátní, a tak se s ním nepřihlásí nikam jinam.

Když jsi říkal, že pokoušet se prolamovat hesla v online formuláři je pomalé, znamená to, že třeba ta aplikace přijímá jen nějaký omezený počet požadavků?

Ano, přesně tak. Odeslání požadavku a odeslání toho formuláře nějakou dobu trvá, zpracování na tom serveru taky. Jenom pro porovnání: u offline útoků, kdy útočník má databázi nějak uložených hesel, mluvíme o rychlostech kolem miliardy pokusů za vteřinu, na rozlousknutí, cracknutí hesla.

V případě pomalejších tzv. password algoritmů na ukládání hesel jsou to tisícovky pokusů za vteřinu. To je pořád mnohem víc, než zvládne například přihlašovací formulář Googlu. Navíc se online pokus dá jednoduše detekovat. Když se někdo snaží přihlásit na Špačka tisíci pokusů za minutu, je to podezřelé a firmy to umí poznat a třeba včas zastavit nebo tam šoupnout captchu a podobně.

Dobře, tak se nebudeme bavit o tom, kolik má mít silné heslo znaků. Mluvil jsi o potřebě unikátnosti. Já jsem se i díky tobě naučil používat správce hesel, password manager. V mém případě jde o 1Password a jsem s tou službu

strašně spokojený. A u správců hesel se vždycky říká, že stačí vytvořit jedno dobré, silné hlavní heslo a pak už na jednotlivých službách generovat náhodná seskupení písmen, číslic a znaků, protože tato hesla už si vlastně pamatovat nemusím, pamatuje si to za mě password manager. O to důležitější je ale to hlavní heslo. Měl bys u něj nějaká doporučení, jak má vypadat nebo jak si ho vytvořit? Pamatuji si, že jsi před lety popisoval, že to může být třeba věta složená z několika náhodně vybraných slov tak, aby si ji člověk dokázal zapamatovat. To pořád platí?

Ano. Nejdřív teda gratuluju k pěkné kličce, jak jsme se k tomu tématu zase vrátili, dobrá práce, přišels na mě od lesa (smích). A ano, heslo do správce hesel je velmi důležité, protože pod ním jsou pak uložená ta další hesla. A jak máme jenom jedno a jak si jich nemusíme pamatovat milión, může být o dost složitější. Může to být nějaký shluk náhodných slov, který se pamatuje trošku líp než dvacet náhodně vytvořených znaků.

Já jsem si třeba tady teď náhodně vygeneroval heslo z šesti anglických slovíček, která jsou náhodně vybraná ze slovníku o asi šedesáti tisících slov. Jsou náhodně seřazená za sebou a poměrně dobře, s trochou tréninku, se dají pamatovat. Je to silné heslo, protože počet kombinací je tak velký, že by to nikdo ani nezkoušel odhadnout. Samozřejmě, pokud bych si za heslo zvolil „skákal pes přes oves“, tak to tak silné není, protože je to předvídatelné.

Opravdu útočníci zkouší, jestli se v heslech nevyskytují tahle známá slovní spojení?

Ano, je to tak. Šance, že někdo použije heslo „Pepíček92“ a „skákalpespřesoves“, je v podstatě stejná. Samozřejmě, plus mínus nějaké desítky procent, ale to tady není důležité. Důležité je to, že víme, že je lidé používají a útočníci to ví taky a vyzkouší je. V jednom článku, kde jsem taky psal o heslech, jsem třeba psal o tom, jak se mi podařilo cracknout heslo se slovy „kobyla má malý bok“. To je podobný případ. Prostě lidi často slyší, že mají používat větu, tak použijí větu (smích).

Tolik tedy letem světem k heslům. Pojďme dál: Česká bankovní asociace na konci srpna v rámci kampaně, která má lidi učit, jak se chovat na internetu bezpečně, zveřejnila svůj Kybertest. Na základě konkrétních situací se v něm snaží lidem ukázat různá hrozící nebezpečí. Říkal jsem si, že by sis ho mohl takhle při našem rozhovoru vyzkoušet. A na základě testu bychom se mohli dostat k dalším tématům.

Pamatuješ si, jak před několika lety Česká bankovní asociace vydala nějakou ročenku nebo co a já jsem se k tomu nějak vyjadřoval?

No, to byl právě ten tvůj článek z roku 2019, který jsi pro Lupu psal, takže se nám to takhle hezky zacyklilo.

A všiml sis, že oni to pak přestali vydávat (smích)?

Tak ten článek byl dost kritický (smích). Pojďme na ten Kybertest. Já si ho spustím paralelně s tebou. Na začátku chce nějaké údaje, jestli jsme muž, nebo žena a kolik nám je přibližně let. Pak je tady obrázek mobilního telefonu, který se chce připojit k veřejné Wi-Fi. Jsou tady na výběr různé možnosti a člověk má odhadnout, která z nich by mohla být bezpečná. Když jsem si ten test zkoušel poprvé, říkal jsem si, že bych neklikl ani na jednu, protože všechny vypadají podezřele. Na tohle téma jsem s tebou chtěl stejně mluvit. Nedávno jsme na Lupě měli zprávu o průzkumu, který varoval před používáním služeb, jako je třeba internetové bankovnictví, právě přes veřejné Wi-Fi sítě. Ty jsi před tím taky před lety hodně varoval. Na konferencích jsi dělával takové pokusy, že jsi zřídil svoji Wi-Fi a pak jsi na ní odchytával informace o připojených lidech. V tomhle případě se situace změnila?

Ano, změnila se zásadně, už takové přednášky nedělám (smích). Nástup šifrování na webu, tedy HTTPS, byl zhruba od roku 2015 razantní, a to je ještě slabé slovo (na této stránce najdete trendy u prohlížeče Google Chrome a tady u Firefoxu). Takže tady se situace hodně změnila. Běžné stránky, e-maily, Lupa a podobně, tam, kde zadávám osobní informace – a nemusí to být jméno a heslo, ani osobní údaje podle nějakého zákona, ale i třeba nějaký můj komentář v diskusi, tak ty jsou přes HTTPS chráněné. Takže před veřejnými Wi-Fi nevaruju, a naopak se dnes snažím říkat, klidně se na veřejnou síť připojte, protože prostě ty věci jsou šifrované.

Pokud bych se připojil na veřejnou Wi-Fi a přihlásil se přes bankovní aplikaci do internetového bankovnictví a někdo mi tam odchytil moje přihlašovací údaje, tak by to bylo fakt špatné. Ale ne kvůli té Wi-Fi, ale protože by ta aplikace byla špatně napsaná.

Když se připojuju na veřejnou Wi-Fi, stejně o ní nevím o moc víc než u neveřejné Wi-Fi zamčené za loginem a heslem. I za ní se může schovávat nějaký Špaček. Prostě přijdu do hospody a zeptám se, jaké mají heslo na Wi-Fi. Oni mi řeknou, že to je síť „U trech soudku“ a heslo je „tripiva“. A já si pak zřídím Wi-Fi „U trech soudku SUPER SPEED“ a dám na ni stejné heslo a lidi se na ni taky připojí. Rozdíl mezi nezabezpečenou veřejnou sítí a zabezpečenou sítí prostě nedokážu na první pohled poznat. Rozhodně to není tak, že jedna vyžaduje heslo a druhá ne.

U veřejných Wi-Fi, ať je provozuje kdokoli, může být někdy možné něco odchytit z DNS dotazů, i když i v téhle oblasti je už dnes pokrok: DNS over HTTPS a podobně. Nějaká analýza by se z těch dat dala udělat, ale nikdo se nedokáže dostat k tomu, co odesílám ve formulářích, jméno, heslo, komentáře a tak dál. Nevidí to, co mám v internetovém bankovnictví, nevidí příkazy, nic takového, jenom může vidět, že jsem se připojil k bance, ale to je všechno.

Jak Michal Špaček v Kybertestu České bankovní asociace dopadl a jak jej hodnotí? Proč by z něj nebyl dobrý zločinec? A jak vypadá budoucnost bez hesel podle představ FIDO Alliance a velkých technologických firem? Poslechněte si celý rozhovor jako podcast:

33. Internetový zločin narůstá. Podvodníci toužili i po příspěvcích na děti

Online ● boleslavsky.denik.cz (Regionální zprávy) ● 5. 9. 2022, 13:30

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)** ● Autor: **Vilém Janouš**

Dosah: 965 223 ● GRP: 10.72 ● OTS: 0.11 ● AVE: 852228.93 Kč

Odkaz: https://boleslavsky.denik.cz/zpravy-z-ceska/internetovy-zlocin-narusta.html

Na jednoho poškozeného klienta připadá škoda přes 160 tisíc korun. Ilustrační foto | *Foto: Shutterstock*

„Pokud se necháte na internetu napálit, tak téměř jistě své peníze neuvidíte v té výši, o kterou jste přišli. Možná, když budete mít štěstí, se vám vrátí část, ale většinou ta menší," uvedl náměstek policejního prezidenta Tomáš Kubík.

Upozornil, že tato trestná činnost narůstá, neboť na internet se přesouvá řada činností. Stejně se tam pak přesouvají zloději. Naposledy se snažili získat data příjemců pětitisícového příspěvku na děti. „Lidem chodily podvodné SMS zprávy, aby lidé daly svá data ke svým účtům s tím, že jim pak budou příspěvky na účet chodit automaticky," uvedla jeden z příkladů kybernetické kriminality z poslední doby výkonná ředitelka České bankovní asociace Monika Zahálková.

Krádeže na internetu: Zloději už letos ukradli tolik, co za celý loňský rok

PŘEČÍST ČLÁNEK ›

Vzrůstající aktivitu zločinců na síti dokládají nejnovější čísla. „Jen za posledních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky narostly hlavně podvodné telefonáty, takzvaný vishing, které patří k těm nejzákeřnějším," řekla Zahálková.

Terčem může být každý

Kubík varoval, že pachatelé jsou sociální inženýři, kteří vědí, na jakou skupinu lidí se zaměřit. „Terčem útoku může být opravdu každý. Iluzorní je se domnívat, že když nemám nic na účtu, tak nemůžu o nic přijít. Jakmile ale dám někomu své údaje, tak si ten člověk na vás sjedná úvěr a další peněžní produkty, které ty banky nabízejí, a ještě vás dostane do dluhů," doplnil.

V mobilech řádí Triada. Trojský kůň umí lidem krást peníze přímo z účtů

PŘEČÍST ČLÁNEK ›

Bankovní asociace proto rozjela kampaň s názvem #nePINdej!, která má na nebezpečí číhající na internetu upozorňovat. Je přitom zaměřená na lidi od 12 let až po seniory. Vychází totiž z toho, že kybernetické kriminalita se už dávno nezaměřuje pouze na starší a osamělé lidi, ale obětí se může stát opravdu každý bez ohledu na věk a vzdělání.

Na internetové adrese www.kybertest.cz si lidé mohou osvojit dovednosti, jak internetovým zlodějům nenaletět.

Základní rady, jak nenaletět zlodějům na internetu

1. Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami v online podvodech.
2. Nikdy se nenech od pachatele do ničeho tlačit a vše pečlivě promysli.
3. Předvídej. Jakmile je zpráva, e-mail, SMS nebo telefonát neočekávaný, tak je podezřelý.
4. Vždy se zamysli nad tím, kam vypisuješ citlivé údaje nebo posíláš peníze.
5. Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
6. Pamatuj si, že pachatel dokáže napodobit jakékoliv telefonní číslo či e-mailovou adresu.
7. Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
8. Nedávej kupujícímu na inzertních portálech citlivé údaje z tvé platební karty, nepotřebuje je.

Zdroj: Kybertest

34. #nePINdej!

Online ● policie.cz (Jiné) ● 5. 9. 2022, 14:51

Dosah: 20 667 ● GRP: 0.23 ● OTS: 0.00 ● AVE: 19996.45 Kč

Odkaz: https://www.policie.cz/clanek/or-melnik-zpravodajstvi-nepindej.aspx

ZPRAVODAJSTVÍ

Úvodní strana / Útvary Policie ČR / Krajská ředitelství policie / Středočes

Policie České republiky – KŘP Středočeského kraje

#nePINdej!

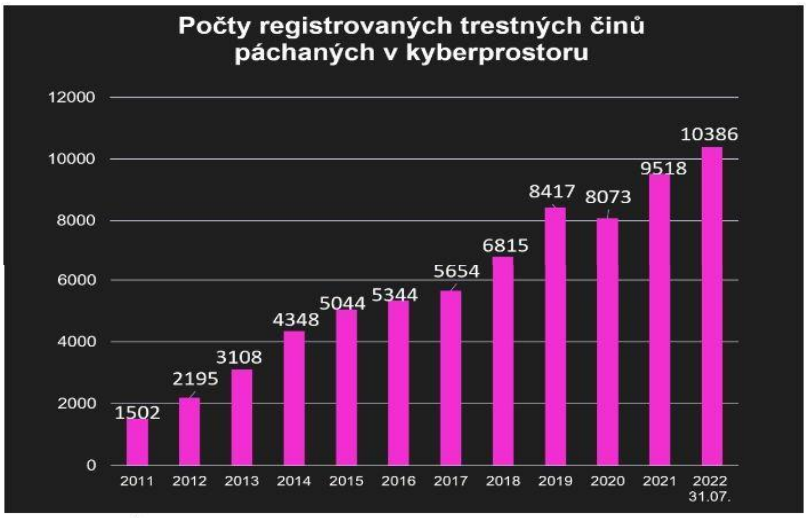
MĚLNICKO - Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů.

Police ČR se dnešním dnem připojuje k rozsáhlé vzdělávací kampani České bankovní asociace a dalších partnerů, která upozorňuje na sílící nebezpečí podvodů na internetu.

Jak vyplývá z dat České bankovní asociace získaných od jejích členských bank, na jednoho poškozeného klienta připadá průměrná škoda ve výši 161 500 korun. U vishingu, neboli případů podvodného navolávání, jsou částky až čtvrtmilionové.

Klíčovým prvkem kampaně s názvem **#nePINdej!** (kreativní tvorba ze slov PIN nedej) je interaktivní vzdělávací **www.kybertest.cz**, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. Kybernetická kriminalita již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Kampaň proto cílí na širokou veřejnost počínaje dětmi a mladistvými přes dospělé až na seniory. *„Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na nejstarší spoluobčany,"* vysvětluje **Tomáš Trachta, člen představenstva společnosti itego, a.s.**, která pro ČBA kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně.

V kybertestu jsou simulovány podvodné SMS, zobrazovací okna k připojení k WIFI sítím, phishingové emaily, zvukové nahrávky podvodných telefonů a mnohé další, tak, aby si je každý uživatel moderních technologií mohl bezpečně vyzkoušet. Testové otázky byly připravovány odborníky na základě reálných případů, jimiž se podvodníci snaží své oběti nachytat. Kampaň #nePINdej! patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají. *„Zároveň bude na sociálních sítích i v dalších kanálech aktivizovat veřejnost k tomu, aby si ve speciálně vytvořené online aplikaci otestovala své schopnosti obstát před kyberútoky,"* říká **Monika Zahálková, výkonná ředitelka České bankovní asociace**.



Počty registrovaných TČ páchaných v kyberprostoru

Pachatelé se při těchto útocích snaží překonávat zejména lidský faktor a pod nejrůznějšími legendami využívají nátlaku, strachu a časové tísně pro záchranu peněz nebo pro realizaci finanční transakce. Mezi nejčastější podvodné legendy patří:

Podvodné navolávání:

- Pachatelé se vydávají například za bankéře, policisty, pracovníky technické podpory a snaží se z lidí pod vlivem strachu vylákat peníze, nebo vzdálený přístup do zařízení oběti, který následně zneužije.

Nabídka výhodných investic:

- Přesvědčivá lákavá reklama a manipulativní jednání. Cílem pachatele je vylákat z oběti co možná nejvíce finančních prostředků a využívá k tomu přirozenou ziskuchtivost každého z nás.

Reverzní inzertní podvody:

- Pachatel zareaguje na váš inzerát. Podstrčí vám fiktivní platební bránu, kde vyplníte citlivé bankovní údaje a místo peněz za inzerované zboží přicházíte o všechny úspory.

Podvody typu Nigerijské dopisy:

- Princip, který funguje už více jak 100 let. Pachatelé sázejí na kvantitu. Vždy se najde někdo, kdo se nechá nachytat na slibovanou cennou zásilku nebo domnělou pomoc. Často zde hraje velkou roli láska.

Klasické podvody typu phishing a smishing:

- Stále dokonalejší a složitě rozpoznatelné podvodné emaily a SMS nabídky. Na první pohled již nenajdeme podezřelé znaky.

Kromě tradičních podvodných e-mailů, SMS a již zmíněného vishingu se stále častěji setkáváme s podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze. *„Loňskou novinkou jsou také tzv. reverzní inzertní podvody, jejichž počet neustále roste. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou,"* objasnil **brig. gen. Tomáš Kubík, náměstek policejního prezidenta pro kriminální policii**.

Kyberkampaň #nePINdej! bude s ohledem na širokou cílovou skupinu probíhat napříč všemi médii – na internetu, v tisku, v České televizi, využita bude i tištěná reklama – formou letáků na pobočkách České pošty –, a pevné reklamní plochy ve vlacích a na nádražích Českých drah, ale i na bankomatech bank působících na českém trhu. Společnost O2 pak kampaň podpoří SMS zprávami s výzvou k účasti na testu. Ze sociálních sítí bude kromě standardních kanálů (Facebook, LinkedIn, Twitter, Instagram) nově využit i TikTok. Kampaň podpoří na svých profilech i influencer Martin „Mikýř" Mikyska.

Základní rady, jak nenaletět

- Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.
- Vyzkoušej si **www.kybertest.cz** a zjisti, kde máš mezery. Buď připraven.

plk. Zuzana Pidrmnaová
vedoucí oddělení prevence

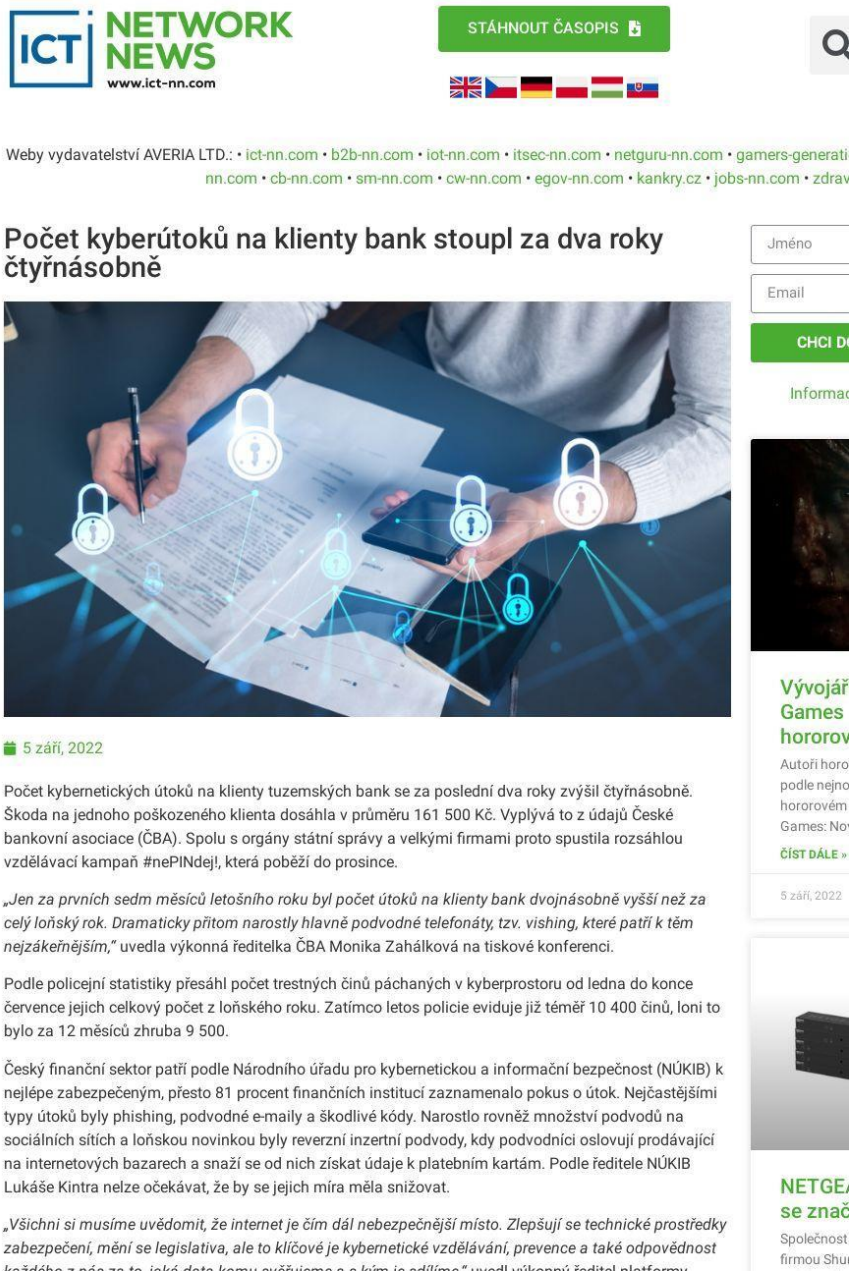
35. Počet kyberútoků na klienty bank stoupl za dva roky čtyřnásobně

Online ● cz.ict-nn.com (IT / Technologie) ● 5. 9. 2022, 15:35

Vydavatel: **AVERIA LTD., organizační složka (cz-28972651)** ● Rubrika: **ICT SECURITY**

Dosah: 898 ● GRP: 0.01 ● OTS: 0.00 ● AVE: 5843.16 Kč

Odkaz: https://cz.ict-nn.com/pocet-kyberutoku-na-klienty-bank-stoupl-za-dva-roky-ctyrnasobne/



ICT NETWORK NEWS
www.ict-nn.com

STÁHNOUT ČASOPIS

Weby vydavatelství AVERIA LTD.: • ict-nn.com • b2b-nn.com • iot-nn.com • itsec-nn.com • netguru-nn.com • gamers-generati nn.com • cb-nn.com • sm-nn.com • cw-nn.com • egov-nn.com • kankry.cz • jobs-nn.com • zdrav

Počet kyberútoků na klienty bank stoupl za dva roky čtyřnásobně

5 září, 2022

Počet kybernetických útoků na klienty tuzemských bank se za poslední dva roky zvýšil čtyřnásobně. Škoda na jednoho poškozeného klienta dosáhla v průměru 161 500 Kč. Vyplývá to z údajů České bankovní asociace (ČBA). Spolu s orgány státní správy a velkými firmami proto spustila rozsáhlou vzdělávací kampaň #nePINdej!, která poběží do prosince.

„Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším," uvedla výkonná ředitelka ČBA Monika Zahálková na tiskové konferenci.

Podle policejní statistiky přesáhl počet trestných činů páchaných v kyberprostoru od ledna do konce července jejich celkový počet z loňského roku. Zatímco letos policie eviduje již téměř 10 400 činů, loni to bylo za 12 měsíců zhruba 9 500.

Český finanční sektor patří podle Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) k nejlépe zabezpečeným, přesto 81 procent finančních institucí zaznamenalo pokus o útok. Nejčastějšími typy útoků byly phishing, podvodné e-maily a škodlivé kódy. Narostlo rovněž množství podvodů na sociálních sítích a loňskou novinkou byly reverzní inzertní podvody, kdy podvodníci oslovují prodávající na internetových bazarech a snaží se od nich získat údaje k platebním kartám. Podle ředitele NÚKIB Lukáše Kintra nelze očekávat, že by se jejich míra měla snižovat.

„Všichni si musíme uvědomit, že internet je čím dál nebezpečnější místo. Zlepšují se technické prostředky zabezpečení, mění se legislativa, ale to klíčové je kybernetické vzdělávání, prevence a také odpovědnost

Jméno
Email
CHCI D
Informac

Vývojář Games hororov
Autoři horo podle nejno hororovém Games: No
ČÍST DÁLE »
5 září, 2022

NETGE se znač
Společnost firmou Shu

každého z nás za to, jaká data komu svěřujeme a s kým je sdílíme," uvedl výkonný ředitel platformy Kybez Michal Řezáč.

Na rostoucí nebezpečí podvodů na internetu má upozornit rozsáhlá vzdělávací kampaň. Klíčovým prvkem kampaně je interaktivní vzdělávací Kybertest na stránkách www.kybertest.cz. Test zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. Kybertest má několik variant, které simulují nejčastější podvodné praktiky podle různých věkových skupin. *„Jiné otázky se tedy generují pro teenagery a jiné pro seniory. Stejně tak jako útoky hackerů. Jiné praktiky zkoušejí na mladší generaci, jiné pak na starší a nejstarší spoluobčany,"* dodal člen představenstva společnosti itego, která test vytvořila, Tomáš Trachta.

Do kampaně jsou vedle České bankovní asociace zapojeni NÚKIB, Policie ČR, itego, Cisco, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy. Mediálními partnery jsou Česká televize, Seznam Zprávy, Deník a Cinestar.

Zdroj: allnews.cz

Foto: Shutterstock

Zdroj: IT SECURITY NETWORK NEWS

ICT SECURITY

PŘEDCHOZÍ
Flotila popelářských vozů na vodíkový pohon nasazená v Evropě

DALŠÍ
NETGEAR navázal partnerství se značkou Shure

Napsat komentář

Pro přidávání komentářů se musíte nejdříve přihlásit.

audio zaříz
instalaci pr
přepínačů N

ČÍST DÁLE »

5 září, 2022

Flotila p
vodíkov
Evropě

Společnost
vodíkové sk
10člennou
vozů nasaz
Nizozemsk

ČÍST DÁLE »

5 září, 2022

36. Kybernetických útoků dramaticky přibývá. ČBA proto spouští vzdělávací kampaň #nePINdej!

Online ● i60.cz (Jiné) ● 5. 9. 2022, 15:49

Vydavatel: **i60 Publishers, s.r.o. (cz-24214868)**

Dosah: 16 724 ● GRP: 0.19 ● OTS: 0.00 ● AVE: 18532.40 Kč

Odkaz: https://www.i60.cz/clanek/detail/31148/kybernetickych-utoku-dramaticky-pribyva-cba-proto-spousti-vzdelavaci-kampan-nepindej

Ilustrace: Česká bankovní asociace

Kybernetických útoků dramaticky přibývá. ČBA proto spouští vzdělávací kampaň #nePINdej!

5. 9. 2022

Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů a na jednoho poškozeného klienta je to v průměru 161 500 korun. Vyplynulo to z dat

České bankovní asociace (ČBA), získaných od jejích členských bank.

ČBA proto ve spolupráci s orgány státní správy a s klíčovými firmami českého byznysu spouští rozsáhlou celonárodní vzdělávací kampaň #nePINdej!

„Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším. Zatímco před dvěma lety se jejich počet pohyboval v nízkých stovkách, letos mluvíme již o desítkách tisíc. A narostla i jejich úspěšnost. Téměř každý druhý podvodný telefonát v současné době bohužel končí škodou pro klienta. Průměrné částka, o kterou klienti při těchto útocích přijdou, je přitom dost vysoká, zhruba čtvrt milionu korun," uvedla Monika Zahálková, výkonná ředitelka České bankovní asociace. Její slova potvrzuje i Lukáš Kintr, ředitel Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). *„Žijeme v digitální době, která nám mnohé věci usnadňuje, ale také přináší mnohá rizika, a mezi ně patří i rostoucí počet různých kyberútoků. Detekujeme vysoké počty nejen podvodných telefonátů, ale i textových zpráv či e-mailů, a nelze očekávat, že by se jejich míra měla snižovat. Nejlepší obranou proti těmto pokusům nadále zůstává obecná osvěta, tedy informovanost a poučenost veřejnosti, aby byli lidé schopni vishing a podobné snahy rozpoznat,"* upřesňuje Lukáš Kintr.

Přibývá také způsobů, jimiž se podvodníci snaží své oběti nachytat. Kromě tradičních podvodných e-mailů, SMS a již zmíněného vishingu se stále častěji setkáváme s podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze. *„Loňskou novinkou jsou také tzv. reverzní inzertní podvody, jejichž počet neustále roste. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou,"* objasnil brig. gen. Tomáš Kubík, náměstek policejního prezidenta pro kriminální policii.

#nePINdej! – celonárodní vzdělávací kampaň v oblasti kyberbezpečnosti

Kybernetická kriminalita také již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Česká bankovní asociace proto spouští rozsáhlou vzdělávací kampaň, která má upozornit na sílící nebezpečí podvodů na internetu. Pod názvem #nePINdej! představí nejčastější kybernetické útoky a formou hravého testu na www.kybertest.cz naučí, jak jim nenaletět. Kampaní chce ČBA oslovit širokou veřejnost – mladistvé od 12 let, dospělé i seniory.

Klíčovým prvkem kampaně #nePINdej! je interaktivní vzdělávací Kybertest, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. *„Název #nePINdej! funguje jako slovní hříčka a je vtipnou výzvou, aby si lidé dávali pozor na své citlivé údaje a chránili své peníze ve světě internetu. Zároveň bude na sociálních sítích i v dalších kanálech aktivizovat veřejnost k tomu, aby si ve speciálně vytvořené online aplikaci otestovala své schopnosti obstát před kyberútoky,"* říká Monika Zahálková, výkonná ředitelka České bankovní asociace.

Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. *„Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na nejstarší spoluobčany,"* vysvětluje Tomáš Trachta, člen představenstva společnosti itego, a.s., která pro ČBA Kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně. Po spuštění testu dostane každý jeho účastník virtuální peníze do „hry", které musí před podvodnými útoky co nejlépe ochránit. Po každé otázce se lidé dozvědí správné řešení, mohou se z něj tak poučit a dalšímu simulovanému útoku následně nenaletět. *„Naším cílem není lidi nachytat a ukázat jim, jak špatně se v kyberprostoru pohybují. Naším cílem je především vzdělat a naučit co nejvíce občanů, jak praktiky podvodníků odhalit a jak se nenechat hackery okrást,"* vysvětluje Monika Zahálková.

Kampaň #nePINdej! zcela jistě patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají. Kromě České bankovní asociace, která je realizátorem projektu, jsou do kampaně zapojeny Policie České republiky, Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), itego, a.s., CISCO, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy. Mediálními partnery jsou Česká televize (hlavní mediální partner), Seznam Zprávy, Deník a Cinestar.

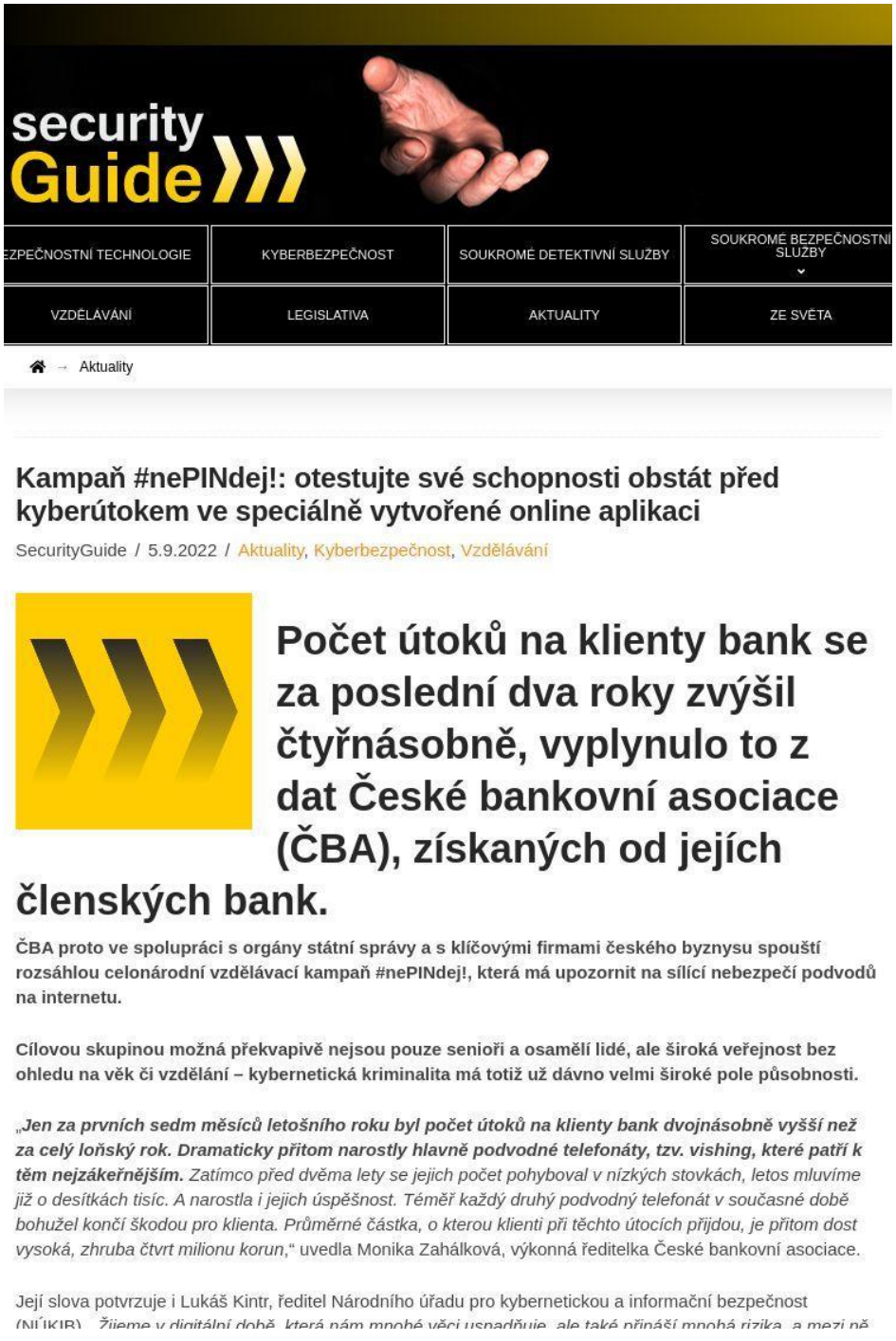
37. Kampaň #nePINdej!: otestujte své schopnosti obstát před kyberútokem ve speciálně vytvořené online aplikaci

Online ● securityguide.cz (IT / Technologie) ● 5. 9. 2022, 17:41

Rubrika: **Aktuality**

Dosah: 874 ● GRP: 0.01 ● OTS: 0.00 ● AVE: 5013.22 Kč

Odkaz: https://securityguide.cz/kampan-nepindej-otestujte-sve-schopnosti-obstat-pred-kyberutokem-ve-specialne-vytvorene-online-aplikaci/



(NÚKIB). „Žijeme v digitální době, která nám mnohé věci usnadňuje, ale také přináší mnoho rizik, a mezi ně patří i rostoucí počet různých kyberútoků. Detekujeme vysoké počty nejen podvodných telefonátů, ale i textových zpráv či e mailů, a nelze očekávat, že by se jejich míra měla snižovat. Nejlepší obranou proti těmto pokusům nadále zůstává obecná osvěta, tedy informovanost a poučenost veřejnosti, aby byli lidé schopni vishing a podobné snahy rozpoznat," upřesňuje Lukáš Kintr.

Přibývá také způsobů, jimiž se podvodníci snaží své oběti nachytat. Kromě tradičních podvodných e-mailů, SMS a již zmíněného vishingu se stále častěji setkáváme s podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze. „*Loňskou novinkou jsou také tzv. reverzní inzertní podvody, jejichž počet neustále roste. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou*," objasnil brig. gen. Tomáš Kubík, náměstek policejního prezidenta pro kriminální policii.

#nePINdej! – celonárodní vzdělávací kampaň v oblasti kyberbezpečnosti

Kybernetická kriminalita také již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Česká bankovní asociace proto spouští rozsáhlou vzdělávací kampaň, která má upozornit na sílící nebezpečí podvodů na internetu. Pod názvem #nePINdej! představí nejčastější kybernetické útoky a formou hravého testu na www.kybertest.cz naučí, jak jim nenaletět. Kampaní chce ČBA oslovit širokou veřejnost – mladistvé od 12 let, dospělé i seniory.

Klíčovým prvkem kampaně #nePINdej! je interaktivní vzdělávací kybertest, který zábavnou formou **seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět.** „*Název #nePINdej! funguje jako slovní hříčka a je vtipnou výzvou, aby si lidé dávali pozor na své citlivé údaje a chránili své peníze ve světě internetu. Zároveň bude na sociálních sítích i v dalších kanálech aktivizovat veřejnost k tomu, aby si ve speciálně vytvořené online aplikaci otestovala své schopnosti obstát před kyberútoky*," říká Monika Zahálková, výkonná ředitelka České bankovní asociace.

Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. „*Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na nejstarší spoluobčany*," vysvětluje Tomáš Trachta, člen představenstva společnosti itego, a.s., která pro ČBA kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně. Po spuštění testu dostane každý jeho účastník virtuální peníze do „hry", které musí před podvodnými útoky co nejlépe ochránit. Po každé otázce se lidé dozvědí správné řešení, mohou se z něj tak poučit a dalšímu simulovanému útoku následně nenaletět. „*Naším cílem není lidi nachytat a ukázat jim, jak špatně se v kyberprostoru pohybují. Naším cílem je především vzdělat a naučit co nejvíce občanů, jak praktiky podvodníků odhalit a jak se nenechat hackery okrást*," vysvětluje Monika Zahálková.

Kampaň #nePINdej! zcela jistě patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají. Kromě České bankovní asociace, která je realizátorem projektu, jsou do kampaně zapojeny Policie České republiky, Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), itego, a.s., CISCO, THEIN, Česká pošta, ČEZ, Mastercard, O2 a České dráhy. Mediálními partnery jsou Česká televize (hlavní mediální partner), Seznam Zprávy, Deník a Cinestar.

O České bankovní asociaci

Česká bankovní asociace vznikla v roce 1990 a je dobrovolným sdružením právnických osob podnikajících v oblasti peněžnictví. V současné době sdružuje 34 členů. Rolí asociace je především zastupovat a prosazovat společné zájmy členů, prezentovat roli a zájmy bankovnictví vůči veřejnosti, podílet se na standardizaci postupů v bankovnictví a na vytváření odborných zvyklostí, podporovat harmonizaci bankovní legislativy s legislativou Evropské unie a vyvíjet aktivitu v informativní a školicí oblasti. ČBA je členem Evropské bankovní federace a EMMI.

Zdroj: TZ; JM

38. Kybernetických útoků dramaticky přibývá a jsou stále rafinovanější. ČBA proto spouští celonárodní vzdělávací kampaň #nePINdej!

Online ● casopisczechindustry.cz (Průmysl / Logistika) ● 5. 9. 2022, 20:59

Vydavatel: **STUDIO P+P, s.r.o. (cz-25054562)**

Dosah: 667 ● GRP: 0.01 ● OTS: 0.00 ● AVE: 4327.53 Kč

Odkaz: https://www.casopisczechindustry.cz/products/kybernetickych-utoku-dramaticky-pribyva-a-jsou-stale-rafinovanejsi-cba-proto-spousti-celonarodni-vzdelavaci-kampan-nepindej/

Přinášíme vám informace, které dávají smysl

O nás ▾ Historie ▾ Ekonomika ▾ Ze zahraničí ▾ Zdraví ▾

Informujeme ▾ Zpravodajství ▾ Civilizace ▾ Styl Zrcadlo ▾

ČASOPIS CZECHINDUSTRY

Magazín českého průmyslu, obchodu, dopravy a stavebnictví

Czech Industry

CzechIndustry > Kybernetických útoků dramaticky přibývá a jsou stále rafinovanější. ČBA proto spouští celonárodní vzdělávací kampaň #nePINdej!

Kybernetických útoků dramaticky přibývá a jsou stále rafinovanější. ČBA proto spouští celonárodní vzdělávací kampaň #nePINdej!

Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů a na jednoho poškozeného klienta je to v průměru 161 500 korun. Vyplynulo to z dat České bankovní asociace (ČBA), získaných od jejích členských bank. ČBA proto ve spolupráci s orgány státní správy a s klíčovými firmami českého byznysu spouští rozsáhlou celonárodní vzdělávací kampaň #nePINdej!

Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším. *Zatímco před dvěma lety se jejich počet pohyboval v nízkých stovkách, letos mluvíme již o desítkách tisíc. A narostla i jejich úspěšnost. Téměř každý druhý podvodný telefonát v současné době bohužel končí škodou pro klienta. Průměrné částka, o kterou klienti při těchto útocích přijdou, je přitom dost vysoká, zhruba čtvrt milionu korun,"* uvedla **Monika Zahálková, výkonná ředitelka České bankovní asociace**. Její slova potvrzuje i **Lukáš Kintr, ředitel Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB)** *„Žijeme v digitální době, která nám mnohé věci usnadňuje, ale také přináší mnohá rizika, a mezi ně patří i rostoucí počet různých kyberútoků. Detekujeme vysoké počty nejen podvodných telefonátů, ale i textových zpráv či e-mailů, a nelze očekávat, že by se jejich míra měla snižovat. Nejlepší obranou proti těmto pokusům nadále zůstává obecná osvěta, tedy informovanost a poučenost veřejnosti, aby byli lidé schopni vishing a podobné snahy rozpoznat,"* upřesňuje **Lukáš Kintr**

Přibývá také způsobů, jimiž se podvodníci snaží své oběti nachytat. Kromě tradičních

podvodných e-mailů, SMS a již zmíněného vishingu se stále častěji setkáváme s podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze. *„Loňskou novinkou jsou také tzv. reverzní inzertní podvody, jejichž počet neustále roste. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou,"* objasnil **brig. gen. Tomáš Kubík, náměstek policejního prezidenta pro kriminální policii**.

Kybernetická kriminalita také již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Česká bankovní asociace proto spouští rozsáhlou vzdělávací kampaň, která má upozornit na sílící nebezpečí podvodů na internetu. Pod názvem #nePINdej! představí nejčastější kybernetické útoky a formou hravého testu na www.kybertest.cz naučí, jak jim nenaletět. Kampaní chce ČBA oslovit širokou veřejnost – mladistvé od 12 let, dospělé i seniory.

#nePINdej!

Klíčovým prvkem kampaně #nePINdej! je interaktivní vzdělávací Kybertest, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. *„Název #nePINdej! funguje jako slovní hříčka a je vtipnou výzvou, aby si lidé dávali pozor na své citlivé údaje a chránili své peníze ve světě internetu. Zároveň bude na sociálních sítích i v dalších kanálech aktivizovat veřejnost k tomu, aby si ve speciálně vytvořené online aplikaci otestovala své schopnosti obstát před kyberútoky,"* říká **Monika Zahálková, výkonná ředitelka ČBA**.

Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. *„Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na nejstarší spoluobčany,"* vysvětluje **Tomáš Trachta, člen představenstva společnosti itego, a.s.**, která pro ČBA Kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně. Po spuštění testu dostane každý jeho účastník virtuální peníze do „hry", které musí před podvodnými útoky co nejlépe ochránit. Po každé otázce se lidé dozvědí správné řešení, mohou se z něj tak poučit a dalšímu simulovanému útoku následně nenaletět. *„Naším cílem není lidi nachytat a ukázat jim, jak špatně se v kyberprostoru pohybují. Naším cílem je především vzdělat a naučit co nejvíce občanů, jak praktiky podvodníků odhalit a jak se nenechat hackery okrást,"* vysvětluje **Monika Zahálková**.

Kampaň #nePINdej! zcela jistě patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají. (5.9.2022)

39. Tady máte 100 tisíc korun. Dokážete je uchránit před podvodníky?

Online ● fzone.cz (IT / Technologie) ● 6. 9. 2022, 10:35

Vydavatel: **24net s.r.o. (cz-24854280)** ● Autor: **Ondřej Pohl**

Dosah: 2 331 ● GRP: 0.03 ● OTS: 0.00 ● AVE: 8208.29 Kč

Odkaz: https://fzone.cz/clanky/tady-mate-100-tisic-korun-dokazete-je-uchranit-pred-podvodniky-4813

Tady máte 100 tisíc korun. Dokážete je uchránit před podvodníky?

Ondřej Pohl 06. 09. 2022

Fotografie: Rupixen, unsplash.com

- **Kybertest České bankovní asociace je kvíz, který připomíná hru**
- **Ocitnete se v reálných situacích, kdy na vás budou útočit podvodníci**
- **Cílem je ochránit před nimi vaše úspory a naučit se něco o internetové bezpečnosti**

SOUVISEJÍCÍ ČLÁNKY

Česká spořitelna umožňuje výběr peněz, aniž byste se dotkli bankomatu

Moneta se opírá do digitalizace, nabídne hypotéky online i dětský účet

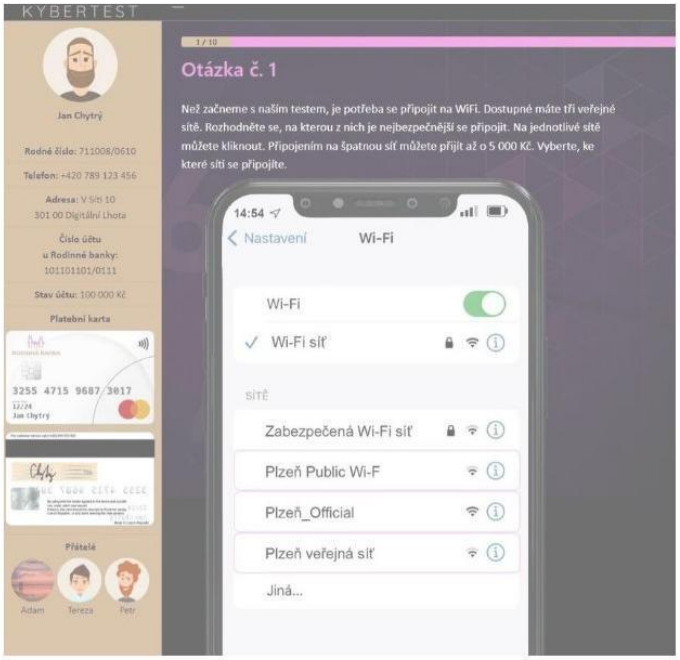
Samsung zkřížil platební kartu a čtečku otisků prstů

Nevíte, co s dlouhými zimními večery? Zkuste honbu za nejvyššími úroky – Glosa

Sberbank nově podporuje Google Pay, Apple Pay se naučí až v příštím roce

Tento zaměstnanec neexistuje. FBI varuje před novým druhem podvodů

Když antispamovým filtrem proklouzne zpráva, ve které vás bohatý nigerijský princ lámanou češtinou nebo angličtinou žádá o pomoc s vyvedením jeho ohromného dědictví ze země, je to spíše úsměvná exkurze do toho, jak neohrabaně internetové podvody začínaly. Jenže i ty se v čase vyvíjejí a jsou čím dál tím zákeřnější. Už nepomůže jednoduché rozlišování podle kvality psaného projevu nebo uvěřitelnosti situace: když čekáte na balíček ze zahraničí, pošta za něj přeci nějaký poplatek vyžadovat bude, nebo ne?



Připojit se k veřejné Wi-Fi může být způsob, jak ušetřit. Anebo přijít o peníze...

Sledovat všechny trendy může být pro obyčejné lidi dost těžké, navíc mnoho podvodných taktik je založeno na tom, že zneužijí nejen vaši neznalost, ale i časovou tíseň. Abyste se mohli o možných nebezpečích poučit, navíc zábavnou formou, spustila Česká bankovní asociace ve spolupráci s odbornými partnery Kybertest.cz.

Jedná se o formu kvízu, který připomíná počítačovou hru. Na začátku dostanete fiktivní identitu a společně s ní i účet se 100 tisíci korunami a platební kartou. V sérii otázek jste pak vystaveni zcela běžným situacím. Kupříkladu hned v první otázce se snažíte najít dostupnou veřejnou Wi-Fi síť. Nabízí se jich hned několik, ale s různými podmínkami pro připojení... Cílem hry je uchránit co nejvíce ze svých virtuálních úspor před podvodníky.

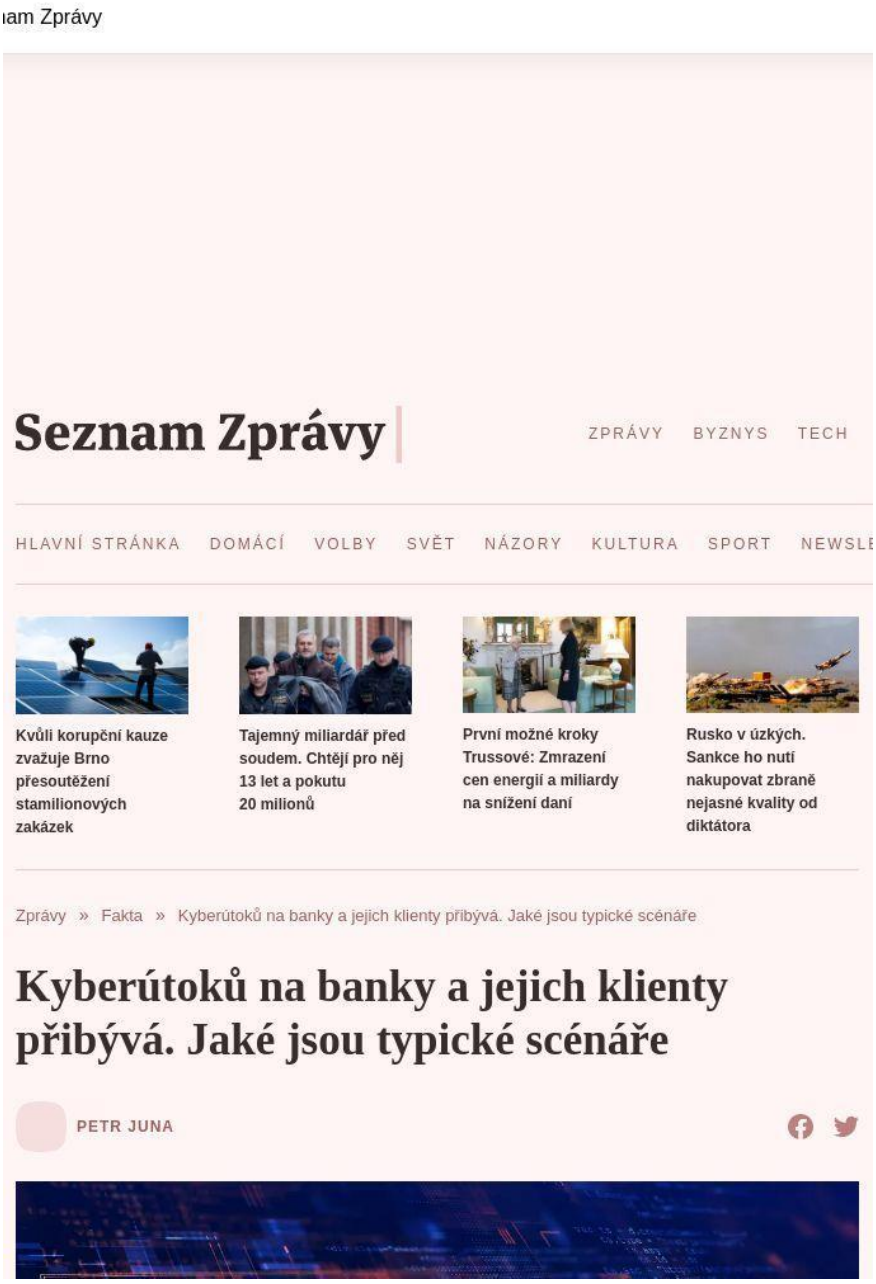
40. Kyberútoků na banky a jejich klienty přibývá. Jaké jsou typické scénáře

Online ● seznamzpravy.cz (Zprávy / Politika) ● 6. 9. 2022, 18:33

Vydavatel: **Seznam.cz, a.s. (cz-26168685)** ● Autor: **Petr Juna**

Dosah: 1 702 492 ● GRP: 18.92 ● OTS: 0.19 ● AVE: 79177.75 Kč ● Interakcí: 111

Odkaz: https://www.seznamzpravy.cz/clanek/fakta-kyberutoku-na-banky-a-jejich-klienty-pribyva-jake-jsou-typicke-scenare-213418



Počet útoků v kyberprostoru prudce roste. (Ilustrační foto)

18:33

K polovině letošního roku hlásí banky čtyřikrát více útoků na své klienty, než jich bylo za celý rok 2020. Každý druhý podvodný telefonát přitom končí poškozením klienta, který v průměru ztrácí přes sto tisíc.

Devět z deseti organizací v Česku, dotázaných Národním úřadem pro kybernetickou bezpečnost, se v roce 2021 setkalo s phishingovým útokem nebo pokusem o něj.

Podle České bankovní asociace zaznamenalo pokus o útok v loňském roce 81 procent bankovních institucí. Na klienty bank jen za prvních sedm měsíců letošního roku směřovalo přes 20 tisíc útoků, za celý rok 2020 to přitom bylo zhruba čtyřikrát méně.

„Dramaticky narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším," popisuje výkonná ředitelka České bankovní asociace Monika Zahálková. Problém je navíc i to, že se zvyšuje úspěšnost útoků.

„Téměř každý druhý podvodný telefonát v současné době bohužel končí škodou pro klienta. Průměrné částka, o kterou klienti při těchto útocích přijdou, je dost vysoká, zhruba čtvrt milionu korun," dodává Zahálková. U jiné metody, phishingu, je průměrná škoda na jednoho klienta 73 tisíc.

„Cílem pachatelů je dostat se nejprve na účet klienta, a ten pak plně převzít pod vlastní kontrolu," vysvětluje pro Seznam Zprávy předseda Komise pro bankovní a finanční bezpečnost ČBA Petr Barák. Způsobů je několik.

„Získají od klienta banky pod různými záminkami jeho přístupové údaje. K účtu si pak s pomocí klienta pod falešnou záminkou spárují i svoje mobilní zařízení jako vlastní autorizační prvek," popisuje Barák. „Popřípadě je sám klient přes například takzvanou ‚vzdálenou plochu' pustí do svého bankovnictví a nechá jim pod záminkou výhodného investování, záchrany ohrožených peněz klienta nebo i jiného důvodu volný přístup ke svým penězům."

Výsledek je podle experta vykradený účet. A to je ještě ta lepší varianta. V té horší si vezmou útočníci na klienta bez jeho vědomí úvěr. „Uvedená částka, o kterou lidé přijdou, je

tedy jen jakýmsi matematickým průměrem. V mnoha případech podvodníci z účtů klientů odčerpají i mnohem vyšší částku," vysvětluje Barák.

Typické scénáře podle Petra Baráka

Vaše peníze jsou v ohrožení = Podvodník se vydává za pracovníka banky. Vyvolá strach na straně klienta tím, že mu tvrdí, že jeho peníze na účtu jsou v ohrožení a pokud je chce zachránit, je tady od toho, aby mu s tím pomohl, a je třeba jednat okamžitě.

Vaše peníze znehodnocuje inflace = Podvodník se vydává za investičního poradce banky / investiční společnosti. Nabízí buď jedinečnou možnost investovat a zhodnotit prostředky na účtu klienta, nebo sděluje klientovi, že se jeho předchozí investice, o které si navíc již sám klient myslel, že mu nic nevydělala, nečekaně zhodnotila a domlouvá s ním způsob jejího vyplacení. Pokud tomu klient uvěří, o své peníze přijde, a to i v druhém případě, kdy je výplata zhodnocené investice podmíněna úhradou nutných poplatků.

Snadný výdělek = Klient banky je vmanipulován do role takzvaného „bílého koně", a to jako osoba, která za úplatu propůjčí svůj účet podvodníkům, kteří přes něj pak legalizují své příjmy z podvodů. Posílají si na takovýto účet odcizené peníze jiných klientů a jeho majitelem si je pak nechávají vybírat v hotovosti a vkládat například do bitcoinmatů – nakupují přes ně různé kryptoměny – nebo si nechávají posílat odcizené prostředky na jiné účty.

Bazarový prodej = Poté, co klient vystaví na některém bazarovém portálu svůj inzerát na prodej zboží, se mu obratem ozve na jeho telefon pachatel v roli zájemce o koupi zboží s tím, že požaduje umožnění úhrady prostřednictvím takzvané „bezpečné platby".

Klient je nasměrován na falešné webové stránky, kde jsou od něj vyžadovány údaje k jeho platební kartě, a to včetně uvedení bezpečnostních prvků platební karty. Pokud klient toto vše vyplní, pachatelé ihned zadávají odchozí platby z jeho účtu s tím, že žádají od klienta pod záminkou, že mu již posílají peníze za zboží, aby jim tyto ve skutečnosti odchozí platby ze svého účtu potvrdil. Pokud klient nečte SMS autorizační zprávy ze své banky a jen potvrzuje to, co mu pachatelé říkají, autorizuje si tím sám podvodné platby a přichází o peníze.

Romance fraud = Nabídky na seznámení se s „důstojníkem US armády, lékařem v Africe, atraktivní dívkou ze zahraničí…", kde je cílem z klienta vylákat postupně stále více peněz za různé nutné výdaje (celní poplatky, poplatky za letenku, poplatky za vyvázání se z vykonávané činnosti

a podobně). Pokud tomu poblouzněný klient/klientka věří a platí, přichází o peníze.

Existuje bohužel velké množství osamělých lidí, kteří ani po upozornění bank, že se jedná o podvod (banka například již zná účet příjemce z minulosti a již ví, že je spojen s tímto typem podvodů), nedbají a peníze odešlou. Případně pokud banka sama peníze odmítne odeslat, jsou schopni si je převést na účet v jiné bance a odeslat je odtud, kde jim je banka ještě sama neodmítne odeslat.

„Těch scénářů je samozřejmě více. Berte tyto jen jako aktuálně nejvíce využívané," říká odborník. „Jak je patrné, hlavní roli sehrává nejen strach a ziskuchtivost, ale i zamilovanost, osamělost, neopatrnost nebo chybějící obyčejný selský rozum, který je mnohdy nahrazen pocitem, že mně se nic takového přece nemůže stát."

Neplatí tedy, že by oběti byly méně finančně gramotné nebo nevzdělané. „Z vlastní praxe znám celou řadu případů, kdy se obětí stali vysokoškolsky vzdělaní lidé středního věku, působící na manažerských pozicích nebo na pozicích v oblasti IT, kde by člověk předpokládal, že se budou chovat obezřetně a nenechají se na tento typ podvodu nachytat. Opak je bohužel pravdou," vysvětluje Barák.

„Žijeme v digitální době, která nám mnohé věci usnadňuje, ale také přináší mnohá rizika. Mezi ně patří i rostoucí počet různých kyberútoků," dodává ředitel NÚKIB Lukáš Kintr. „Detekujeme vysoké počty nejen podvodných telefonátů, ale i textových zpráv či e-mailů, a nelze očekávat, že by se jejich míra měla snižovat. Nejlepší obranou proti těmto pokusům nadále zůstává obecná osvěta, tedy informovanost a poučenost veřejnosti, aby byli lidé schopni vishing a podobné snahy rozpoznat."

I proto spustila ČBA celonárodní vzdělávací kampaň, jejíž součástí je také online interaktivní kybertest. Na něm si mohou uživatelé vyzkoušet, jestli znají základní principy bezpečného chování na internetu.

41. Úspěšný útok v kyberprostoru znamená průměrnou ztrátu 162 tisíc Kč, otestujte si své vědomosti

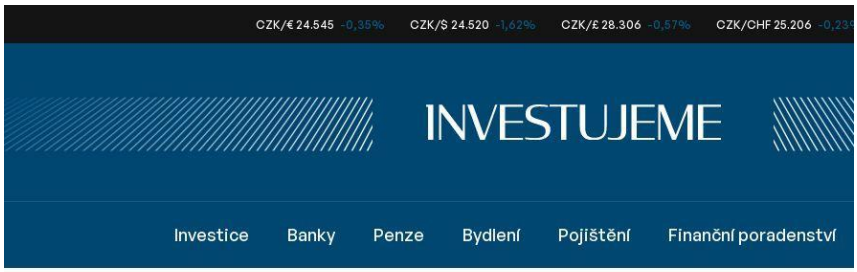
Online ● investujeme.cz (Ekonomika / Finance / Právo) ● 8. 9. 2022, 8:35

Vydavatel: **Fincentrum & Swiss Life Select a.s. (cz-24260444)**

Dosah: 3 096 ● GRP: 0.03 ● OTS: 0.00 ● AVE: 9355.89 Kč ● Interakcí: 1

Odkaz: https://www.investujeme.cz/clanky/uspesny-utok-v-kyberprostoru-znamena-prumernou-ztratu-162-tisic-kc-otestujte-si-sve-vedomosti/

...



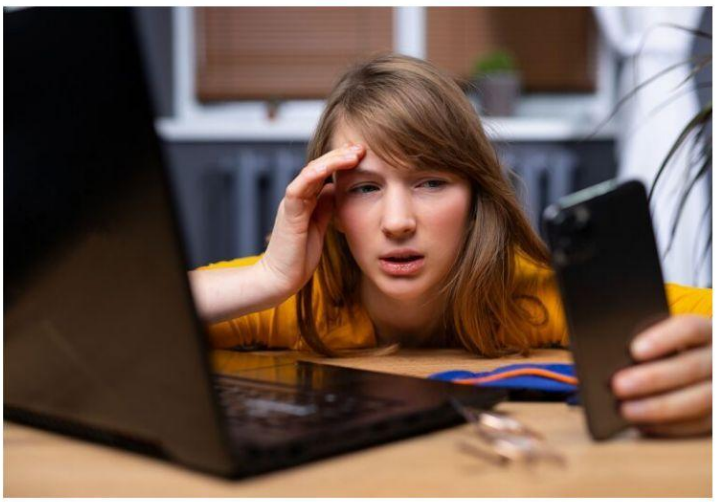
Text: **Redakce**
Foto: Shutterstock
09. 09. 2022

0 komentářů

Úspěšný útok v kyberprostoru znamená průměrnou ztrátu 162 tisíc Kč, otestujte si své vědomosti

FINANČNÍ PORADENSTVÍ

Počet útoků na klienty bank, občany, ale i firmy strmě roste. Narůstající škody registrují banky i policisté. Podvodná jednání mohou mít desítky nejrůznějších scénářů a podob a cílí prakticky na všechny věkové skupiny.



Největší procento kybernetických útoků (téměř 40 %) směřuje do veřejného sektoru, soukromé sféry (21 %) a zdravotnictví (17 %). I když finanční segment patří z hlediska podílu na celkovém počtu útoků k těm méně zasaženým, jde o citlivou oblast, protože případné škody se přímo dotýkají úspor obyvatel.

Banky do bezpečnosti masivně investují

Český finanční sektor patří k nejlépe zabezpečeným. Podle zprávy Národního úřadu kybernetické a informační bezpečnosti za rok 2021 investují banky ve srovnání s jinými institucemi do kyberbezpečnosti nejvyšší procento ze svých rozpočtů a 43 % z nich dokonce plánují letos rozpočet na tuto oblast navýšit. Tyto výdaje souvisí i s tím, že 81 % finančních institucí zaznamenalo v loňském roce nějaký pokus o útok.

Zvyšují se počty útoků i škoda

Zatímco v roce 2020 bylo registrováno zhruba 5000 útoků na klienty bank, loni už to bylo více než 12 000 a letos jen za prvních sedm měsíců roku podvodníci útočili v téměř 21 tisících případech. Vyplynulo to z dat, které banky poskytly České bankovní asociaci.

„Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším. Zatímco před dvěma lety se jejich počet pohyboval v nízkých stovkách, letos mluvíme již o desítkách tisíc. A narostla i jejich úspěšnost. Téměř každý druhý podvodný telefonát v současné době bohužel končí škodou pro klienta," uvedla výkonná ředitelka České bankovní asociace Monika Zahálková.

Průměrné částky, o které klienti při útocích přicházejí, jsou přitom bohužel dost vysoké. Při úspěšném útoku přijde klient v průměru o 161 500 korun. Phishing (podvodné e-maily) přitom přináší škodu kolem 73 tisíc korun u jednoho klienta, u podvodných telefonátů je škoda mnohem vyšší, v průměru čtvrt milionu korun.

Podvodníci přicházejí s novými metodami

Přibývá také způsobů, jimiž se podvodníci snaží své oběti nachytat. Kromě tradičních podvodných e-mailů, SMS a již zmíněného vishingu jsou stále častější podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby, a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze.

Loňskou novinkou jsou také tzv. reverzní inzertní podvody, jejichž počet neustále roste. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu „bezpečnou platbu", tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou.

Proto Česká bankovní asociace spustila minulý týden rozsáhlou kampaň #nePINdej! Ústředním prvkem kampaně je Kybertest.

42. KYBERPODVODY

Tisk ● Katalog, Novinky, Senior pas; str. 4 (Regionální zprávy) ● 9. 9. 2022

Vydavatel: **Senioři České republiky, z. s., Městská organizace Brno (cz-69706824)** ● Rubrika: **PORADNA**

Odkaz: náhled

PORADNA

KYBERPODVODY

Policisté opakovaně upozorňují na silící vlnu podvodů, která probíhá ve virtuálním světě. Denně se jedná o desítky nových případů s velmi podobným scénářem

Nejčastější způsoby podvodů na internetu jsou následující:

Využívání inzertních portálů. Nabízíte například na prodej nějaké zboží. Zkontaktuje vás podvodník, který prý má zájem o nabízené zboží, nicméně preferuje platbu a doručení zboží prostřednictvím přepravní společnosti a pošle vám odkaz. Kliknutí na odkaz vás většinou přesměruje na stránku pro zadání přihlašovacích údajů do vašeho internetového bankovnictví. Pokud dojde k přihlášení, podvodník získá přístup do vašeho internetového bankovnictví a provede neoprávněné transakce.

Falešná technická podpora. Podvodník, vydávající se za pracovníka technické podpory operačního systému vašeho počítače, vás kontaktuje s vymyšleným příběhem o napadení vašeho účtu hackery. Vyžaduje po vás vzdálený přístup k vašemu soukromému počítači, což většinou proběhne přes kliknutí na nějaký zaslaný odkaz. Tento vzdálený přístup mu bohužel umožní ovládání vašeho počítače. Další požadavek podvodníka je vyplnění formuláře, který obsahuje citlivé údaje k vaší platební kartě včetně její platnosti a CVC kódu. Jakmile se k těmto údajům dostane, může provádět z vašeho účtu platby, zřídit úvěr apod.

Výhodná nabídka – investice do kryptoměn. Podvodník od vás vyšle platební údaje nebo získá přístup k vašemu počítači a provede z vašeho účtu neoprávněné transakce.

Falešný bankéř. Podvodník vás telefonicky zkontaktuje s odůvodněním, že si ověřuje vaši žádost o úvěr. Zde se většinou každý ohradí, že žádný úvěr nemá a ani nemá účet u uvedené banky. Podvodník se omluví a sdělí, že informaci předá do banky. Poté následuje další telefonát, kdy se podvodník vydává za pracovníka banky, která vede váš účet. Podvodník vám sdělí, že došlo k napadení vašeho účtu, a je nezbytné nutné vybrat veškerou hotovost. Následuje nabídka převodu peněz na bezpečný účet a zaslání QR kódu na telefon. Tento kód máte poté načíst u bitcoinového bankomatu při vkládání peněz.

Na všechny způsoby podvodů však platí stejné rady a doporučení, jak se nestát obětí kyberpodvodníků:

1. Nikdy nikomu nesdělujte své přihlašovací údaje do internetového bankovnictví ani čísla ze své platební karty. **Banky se na ně neptají, ani zprávami či e-mailem neposílají odkazy na weby, kde jsou vyžadovány!**
2. Při každém vstupu do internetového bankovnictví kontrolujte, zda odpovídá doména přihlašovací stránky. Toto platí vždy, když někam zadáváte své osobní nebo přihlašovací údaje.
3. Sledujte a pečlivě čtěte informace od vaší banky v internetovém bankovnictví.
4. Nereagujte na telefonní hovory, e-maily ani zprávy, kde se vás někdo pokouší vmanipulovat do situace, že jsou vaše finanční prostředky v ohrožení a vy musíte udělat další krok pro jejich záchranu.
5. Nezadávejte ani v aplikaci nepotvrzujte platby, které vám bude diktovat někdo po telefonu, ani nikomu nesdělujte či nepřeposílejte potvrzovací kódy z SMS. Stejně tak nedávejte nikomu vzdálený přístup do vašeho počítače.
6. Myslete na to, že útočník dokáže napodobit jakékoliv telefonní číslo, odesílatele SMS zprávy, ale třeba i e-mailovou adresu.
7. Podvodnou platbu co nejdříve ohlaste na PČR a co nejdříve reklamujte u svého bankovního subjektu.
8. Jakoukoli komunikaci ze strany podvodníka nemažte do doby, než bude zajištěna policejním orgánem.
9. Buďte obezřetní při využívání inzertních portálů. Pečlivě volte způsob platby a ani v těchto případech neklikejte na zaslané odkazy.
10. Mějte aktualizovaný software a antivirus. A to i na mobilním telefonu.
11. V případě pochybností vždy kontaktujte svou banku či volejte 158.

Odhalíte včas, že na vás útočí online podvodníci? Vyzkoušejte si test a poměřte své výsledky s ostatními na **www.kybertest.cz**.

Krajské ředitelství Policie Jihomoravského kraje

6 | NOVINKY Senior Pas | 1/2022 | www.SeniorPasy.cz

SENIOR PASY

SVÁTEK SENIORŮ
slavíme také v Jihomoravském kraji

U příležitosti Mezinárodního dne seniorů, který každoročně připadá na **1. říjnový den**, se po celé České republice konají seniorské oslavy ve formě kulturních událostí nebo společenských setkání. Nejen seniorské organizace připravují sváteční program, jehož rozmanitou formou se snaží seniory potěšit.

Také Jihomoravský kraj se připojuje k těmto oslavám. Již dvanáctý ročník kulturní události Svátek seniorů realizuje v Brně opět na Zelném trhu. Touto tradiční akcí vyjadřuje Jihomoravský kraj seniorům svou úctu a poděkování. Letos se brněnský Svátek seniorů ponese v duchu mezigeneračního propojení. Dopolední pódiový program bude patřit rodinám s dětmi a odpoledne právě seniorům. Můžeme se těšit na hudební vystoupení Bohuše Matuše, sester Marthy a Teny Elefteriadu, Brněnského Valáška a mnohé další.

Slaví i města Znojmo a Hodonín

Jihomoravský kraj pořádá oslavy Svátku seniorů také na dalších místech kraje. Díky spolupráci s okresními městy Znojmo a Hodonín se senioři potěší kulturním programem i v uvedených městech. Vstup na akci je zdarma a podrobný program najdete na webových stránkách **www.svateksenioru.cz**.

Svátek seniorů 2022

BRNO Neděle 18. 9. • 14.00 – 17.00 • Zelný trh (Den zábavy s Rodinnými pasy od 10.00)

ZNOJMO Pondělí 26. 9. • 16.00 - 19.00 • Městské divadlo Znojmo, nám. Republiky 916

HODONÍN Pátek 30. 9. • 16.00 - 21.00 • Dům kultury, Horní Valy 6

SVÁTEK SENIORŮ

Fotografie z oslav v roce 2021

jihomoravský kraj | BRNO | MĚSTO HODONÍN | znojmo | Senior pas | SDC SunDrive

www.SeniorPasy.cz | NOVINKY Senior Pas | 1/2022 | 7

43. #nePINdej!

Online ● mesto-horovice.eu (Regionální zprávy) ● 12. 9. 2022, 13:08

Autor: **Simona Vacherlohnová**

Dosah: 215 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 2223.99 Kč

Odkaz: https://www.mesto-horovice.eu/bezpecne-mesto-1/policie-cr/policie-patra-a-informuje-1/nepindej-1429cs.html

Hořovice

+420 311 545 301
e-podatelna@mesto-horovice.cz

Aktuálně | Město | Městský úřad | Pro občana | Volný čas | Bezpečné město

Bezpečné město
- Policie ČR
- Policie pátrá a informuje
- Kontakty
- Preventivní informace
- POL POINT
- Statistiky kriminality
- Přidejte se k našemu policejnímu týmu
- Prověřte si věci v pátrání
- Městská policie
- Prevence kriminality
- Městský kamerový dohlížecí systém
- Zajímavosti

Rizika a nebezpečí

RIZIKA A NEBEZPEČÍ
Senioři v dopravě
Podle pravidel silničního provozu je chodcem každý, kdo vstoupil na chodník nebo na silnici. Je úplně jedno, zda stojí nebo jde. Chodník je součástí pozemní komunikace. Chodcem je také ten, kdo tlačí nebo táhne sáňky, kočárek,
VÍCE RAD A INFORMACÍ

Mobilní aplikace

V OBRAZE
Vím, co se děje

Sledujte informace

Bezpečné město › Policie ČR › Policie pátrá a informuje › #nePINdej!

#nePINdej!

BEROUNSKO - Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů. Policie ČR se dnešním dnem připojuje k rozsáhlé vzdělávací kampani České bankovní asociace a dalších partnerů, která upozorňuje na sílící nebezpečí podvodů na internetu.

Jak vyplývá z dat České bankovní asociace získaných od jejích členských bank, na jednoho poškozeného klienta připadá průměrná škoda ve výši 161 500 korun. U vishingu, neboli případů podvodného navolávání, jsou částky až čtvrtmilionové.

Klíčovým prvkem kampaně s názvem **#nePINdej!** (kreativní tvorba ze slov PIN nedej) je interaktivní vzdělávací **www.kybertest.cz**, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. Kybernetická kriminalita již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Kampaň proto cílí na širokou veřejnost počínaje dětmi a mladistvými přes dospělé až na seniory. *„Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na nejstarší spoluobčany,“* vysvětluje **Tomáš Trachta, člen představenstva společnosti itego, a.s.**, která pro ČBA kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně.

V kybertestu jsou simulovány podvodné SMS, zobrazovací okna k připojení k WIFI sítím, phishingové emaily, zvukové nahrávky podvodných telefonů a mnohé další, tak, aby si je každý uživatel moderních technologií mohl bezpečně vyzkoušet. Testové otázky byly připravovány odborníky na základě reálných případů, jimiž se podvodníci snaží své oběti nachytat. Kampaň #nePINdej! patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají. *„Zároveň bude na sociálních sítích i v dalších kanálech aktivizovat veřejnost k tomu, aby si ve speciálně vytvořené online aplikaci otestovala své schopnosti obstát před kyberútoky,“* říká **Monika Zahálková, výkonná ředitelka České bankovní asociace**.

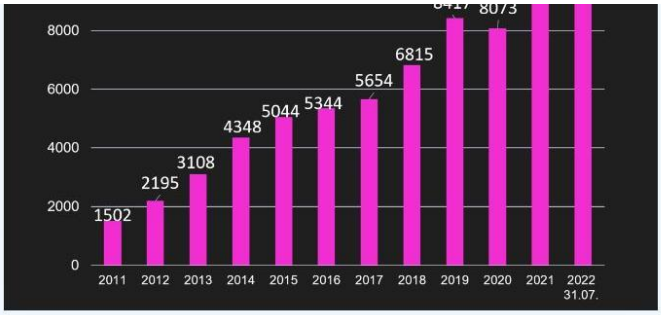
Po Út St Čt Pá So Ne
29 30 31 1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 1 2

Senioři

Zjednodušená verze stránek nejen pro seniory

Náš web

Administrace webu
ic@mkc-horovice.cz
Napište nám!
O tom, co jste na těchto stránkách nenašli, nebo o tom,
co byste našli rádi, možná jinak a jinde...



Počty registrovaných TČ páchaných v kyberprostoru

Pachatelé se při těchto útocích snaží překonávat zejména lidský faktor a pod nejrůznějšími legendami využívají nátlaku, strachu a časové tísně pro záchranu peněz nebo pro realizaci finanční transakce. Mezi nejčastější podvodné legendy patří:

Podvodné navolávání:

- Pachatelé se vydávají například za bankéře, policisty, pracovníky technické podpory a snaží se z lidí pod vlivem strachu vylákat peníze, nebo vzdálený přístup do zařízení oběti, který následně zneužije.

Nabídka výhodných investic:

- Přesvědčivá lákavá reklama a manipulativní jednání. Cílem pachatele je vylákat z oběti co možná nejvíce finančních prostředků a využívá k tomu přirozenou ziskuchtivost každého z nás.

Reverzní inzertní podvody:

- Pachatel zareaguje na váš inzerát. Podstrčí vám fiktivní platební bránu, kde vyplníte citlivé bankovní údaje a místo peněz za inzerované zboží přicházíte o všechny úspory.

Podvody typu Nigerijské dopisy:

- Princip, který funguje už více jak 100 let. Pachatelé sázejí na kvantitu. Vždy se najde někdo, kdo se nechá nachytat na slibovanou cennou zásilku nebo domnělou pomoc. Často zde hraje velkou roli láska.

Klasické podvody typu phishing a smishing:

- Stále dokonalejší a složitě rozpoznatelné podvodné emaily a SMS nabídky. Na první pohled již nenajdeme podezřelé znaky.

Kromě tradičních podvodných e-mailů, SMS a již zmíněného vishingu se stále častěji setkáváme s podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze. *„Loňskou novinkou jsou také tzv. reverzní inzertní podvody, jejichž počet neustále roste. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech*

na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou,“ objasnil **brig. gen. Tomáš Kubík, náměstek policejního prezidenta pro kriminální policii**.

Kyberkampaň #nePINdej! bude s ohledem na širokou cílovou skupinu probíhat napříč všemi médii – na internetu, v tisku, v České televizi, využita bude i tištěná reklama – formou letáků na pobočkách České pošty –, a pevné reklamní plochy ve vlacích a na nádražích Českých drah, ale i na bankomatech bank působících na českém trhu. Společnost O2 pak kampaň podpoří SMS zprávami s výzvou k účasti na testu. Ze sociálních sítí bude kromě standardních kanálů (Facebook, LinkedIn, Twitter, Instagram) nově využit i TikTok. Kampaň podpoří na svých profilech i influencer Martin „Mikýř“ Mikyska.

Základní rady, jak nenaletět

- Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.
- Vyzkoušej si **www.kybertest.cz** a zjisti, kde máš mezery. Buď připraven.

plk. Zuzana Pidrmanová
vedoucí oddělení prevence

Datum vložení: 12. 9. 2022 13:08
Datum poslední aktualizace: 12. 9. 2022 13:10

Autor: nprap. Simona Vacherlohnová

44. #nePINdej!

Online ● policie.cz (Jiné) ● 12. 9. 2022, 13:11

Dosah: 20 667 ● GRP: 0.23 ● OTS: 0.00 ● AVE: 19996.45 Kč

Odkaz: https://www.policie.cz/clanek/sprava-stredoceskeho-kraje-or-beroun-zpravodajstvi-nepindej.aspx

ZPRAVODAJSTVÍ

Úvodní strana / Útvary Policie ČR / Krajská ředitelství policie / Středočes

Policie České republiky – KŘP Středočeského kraje

#nePINdej!

BEROUNSKO - Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů. Policie ČR se dnešním dnem připojuje k rozsáhlé vzdělávací kampani České bankovní asociace a dalších partnerů, která upozorňuje na sílící nebezpečí podvodů na internetu.

Jak vyplývá z dat České bankovní asociace získaných od jejích členských bank, na jednoho poškozeného klienta připadá průměrná škoda ve výši 161 500 korun. U vishingu, neboli případů podvodného navolávání, jsou částky až čtvrtmilionové.

Klíčovým prvkem kampaně s názvem **#nePINdej!** (kreativní tvorba ze slov PIN nedej) je interaktivní vzdělávací **www.kybertest.cz**, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. Kybernetická kriminalita již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Kampaň proto cílí na širokou veřejnost počínaje dětmi a mladistvými přes dospělé až na seniory. *„Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na nejstarší spoluobčany,“* vysvětluje **Tomáš Trachta, člen představenstva společnosti itego, a.s.**, která pro ČBA kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně.

V kybertestu jsou simulovány podvodné SMS, zobrazovací okna k připojení k WIFI sítím, phishingové emaily, zvukové nahrávky podvodných telefonů a mnohé další, tak, aby si je každý uživatel moderních technologií mohl bezpečně vyzkoušet. Testové otázky byly připravovány odborníky na základě reálných případů, jimiž se podvodníci snaží své oběti nachytat. Kampaň #nePINdej! patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají. *„Zároveň bude na sociálních sítích i v dalších kanálech aktivizovat veřejnost k tomu, aby si ve speciálně vytvořené online aplikaci otestovala své schopnosti obstát před kyberútoky,“* říká **Monika Zahálková, výkonná ředitelka České bankovní asociace**.

Pachatelé se při těchto útocích snaží překonávat zejména lidský faktor a pod nejrůznějšími legendami využívají nátlaku, strachu a časové tísně pro záchranu peněz nebo pro realizaci finanční transakce. Mezi nejčastější podvodné legendy patří:

Podvodné navolávání:

- Pachatelé se vydávají například za bankéře, policisty, pracovníky technické podpory a snaží se z lidí pod vlivem strachu vylákat peníze, nebo vzdálený přístup do zařízení oběti, který následně zneužije.

Nabídka výhodných investic:

- Přesvědčivá lákavá reklama a manipulativní jednání. Cílem pachatele je vylákat z oběti co možná nejvíce finančních prostředků a využívá k tomu přirozenou ziskuchtivost každého z nás.

Reverzní inzertní podvody:

- Pachatel zareaguje na váš inzerát. Podstrčí vám fiktivní platební bránu, kde vyplníte citlivé bankovní údaje a místo peněz za inzerované zboží přicházíte o všechny úspory.

Podvody typu Nigerijské dopisy:

- Princip, který funguje už více jak 100 let. Pachatelé sázejí na kvantitu. Vždy se najde někdo, kdo se nechá nachytat na slibovanou cennou zásilku nebo domnělou pomoc. Často zde hraje velkou roli láska.

Klasické podvody typu phishing a smishing:

- Stále dokonalejší a složitě rozpoznatelné podvodné emaily a SMS nabídky. Na první pohled již nenajdeme podezřelé znaky.

Kromě tradičních podvodných e-mailů, SMS a již zmíněného vishingu se stále častěji setkáváme s podvody na sociálních sítích, kdy pachatel může dokonce ukrást identitu reálné osoby a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze. *„Loňskou novinkou jsou také tzv. reverzní inzertní podvody, jejichž počet neustále roste. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou,"* objasnil **brig. gen. Tomáš Kubík, náměstek policejního prezidenta pro kriminální policii**.

Kyberkampaň #nePINdej! bude s ohledem na širokou cílovou skupinu probíhat napříč všemi médii – na internetu, v tisku, v České televizi, využita bude i tištěná reklama – formou letáků na pobočkách České pošty –, a pevné reklamní plochy ve vlacích a na nádražích Českých drah, ale i na bankomatech bank působících na českém trhu. Společnost O2 pak kampaň podpoří SMS zprávami s výzvou k účasti na testu. Ze sociálních sítí bude kromě standardních kanálů (Facebook, LinkedIn, Twitter, Instagram) nově využit i TikTok. Kampaň podpoří na svých profilech i influencer Martin „Mikýř" Mikyska.

Základní rady, jak nenaletět

- Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.
- Vyzkoušej si **www.kybertest.cz** a zjisti, kde máš mezery. Buď připraven.

plk. Zuzana Pidrmanová
vedoucí oddělení prevence

45. #04 ČBA Focus 2022

Online ● cbaonline.cz ((nezařazené)) ● 13. 9. 2022, 11:31

Dosah: 950 ● GRP: 0.01 ● OTS: 0.00 ● AVE: 5241.02 Kč

Odkaz: https://cbaonline.cz/04-cba-focus-2022

46.Česká pošta se zapojila do kampaně nePINdej!

Online ● infodnes.cz (Zprávy / Politika) ● 13. 9. 2022, 13:41

Vydavatel: **M+MP spol. s r.o. (cz-26777134)**

Dosah: 1 845 ● GRP: 0.02 ● OTS: 0.00 ● AVE: 7341.69 Kč

Odkaz: https://www.infodnes.cz/zpravodajstvi/47547-ceska-posta-se-zapojila-do-kampane-nepindej/

InfoDnes | ZPRAVODAJSTVÍ

Vyhledat zprávu

Hlavní přehled | Domácí | Regiony | Krimi | Ekonomika | Kultura | Magazín | Přehled tisku | Přidat zprávu | Arc

InfoDnes.cz » Zpravodajství » Domácí

Česká pošta se zapojila do kampaně nePINdej!

13.09.2022

Klienti České pošty jsou stále častěji vystavování kybernetickým útokům, při nichž je zneužíváno jméno České pošty. Nejčastěji se jedná o podvodné elektronické zprávy či SMS zprávy, které se snaží z jejich adresátů získat různými způsoby peníze nebo přístup k osobním údajům či bankovním účtům. Kromě toho, že Česká pošta dlouhodobě upozorňuje před podobným podvodným jednáním na svých webových stránkách www.ceskaposta.cz, zapojila se také do nové vzdělávací kampaně České bankovní asociace s názvem #nePINdej!

Foto: ČBA

Nová kampaň má upozornit na sílící nebezpečí podvodů na internetu. Pod názvem #nePINdej! představí nejčastější kybernetické útoky a formou hravého testu na www.kybertest.cz naučí, jak jim nenaletět.

V poslední době se množí podvodné e-maily a sms zprávy, které mají adresáty připravit o peníze a k tomu jim poškodit počítač či mobilní telefon. Toto provádí díky zneužívání jména České pošty. Varujeme proto klienty České pošty před podvodnými elektronickými zprávami (phishing), které jsou zasílány z podvodných adres. Tyto podvodné e-mailové zprávy nerozesílá Česká pošta a nemá s nimi nic společného.

Veškeré falešné zprávy, které Pošta obdrží, zveřejňuje na svých webových stránkách jako varování. Na stejném místě jsou také rady a postupy, jak phishingový útok rozpoznat. Na uvedené webové stránky se lze dostat kliknutím na banner umístěný přímo na hlavní stránce webu nebo jej klienti naleznou zde: www.ceskaposta.cz/o-ceske-poste/bezpecnostni-informace.

Kampaň #nePINdej! zcela jistě patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají. Kromě České bankovní asociace, která je realizátorem projektu, a České pošty, jsou do kampaně zapojeny Policie České republiky, Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), itego, a.s., CISCO, Thein Security, ČEZ, Mastercard, O2 a České dráhy. Mediálními partnery jsou Česká televize, Seznam Zprávy, Deník a Cinestar.

Zdroj: Česká pošta

47. Finanční gramotnost Čechů mírně vzrostla. Lépe si vedou starší ročníky

Tisk ● Bankovnictví; str. 5 (Ekonomika / Finance / Právo) ● 14. 9. 2022

Vydavatel: **4H production s.r.o. (cz-28471831)** ● Rubrika: **SPEKTRUM**

Dosah: 12 248 ● GRP: 0.14 ● OTS: 0.00 ● AVE: 79000.00 Kč

Odkaz: náhled

Finanční gramotnost Čechů mírně vzrostla. Lépe si vedou starší ročníky

Index finanční gramotnosti České bankovní asociace (ČBA) vzrostl na 56 bodů. Proti loňsku je to mírné zlepšení o jeden bod. Tři čtvrtiny dotazovaných se obávají rychlého růstu cen a kvůli současné inflaci chtějí šetřit. Velká část však neplánuje naspořené peníze chránit proti inflačnímu znehodnocení. Přispívá k tomu i to, že se nevyznají v investicích a v radách finančních poradců. V souvislosti se začátkem školního roku budou muset tři z deseti rodičů omezit výdaje. Vyplývá to z nového průzkumu ČBA a agentury Ipsos, který probíhal během srpna, a zúčastnilo se ho 1 063 respondentů ve věku 18–79 let.

Částečné potíže v orientaci ve světě financí přiznává naprostá většina Čechů. Ukázaly to výsledky Indexu finanční gramotnosti, který Česká bankovní asociace dlouhodobě sleduje. Jedná se o sadu jedenácti otázek, které se týkají různých oblastí finanční gramotnosti. Největší rozdíl v úspěšnosti pozorujeme u vzdělání. Zatímco lidé s vysokoškolským vzděláním dosáhli 62 bodů, ti se základní školou nebo výučním listem získali pouze 48 bodů. Potíže přitom způsobil hlavně dotaz na výhodnost úvěru, který dokázala správně zodpovědět méně než třetina dotazovaných (31 procent).

„Je vidět, že kromě vzdělání získávají lidé znalosti často i díky letitým zkušenostem, což

potvrzuje fakt, že lepších výsledků dosahovali lidé nad 50 let – v průměru 58 bodů. Celkově je však stále finanční gramotnost v Česku z mého pohledu nedostatečná a lidé selhávají v základních věcech. To má pak za následek větší zranitelnost. Česká bankovní asociace se proto snaží povědomí o financích a finančních produktech zlepšovat řadou vzdělávacích projektů. Nejoblíbenější projekty, mezi které patří Bankéři do škol a celoevropský European Money Quiz, cílí už na děti a kvůli přibývajícím kybernetickým útokům startujeme v září velkou vzdělávací kampaň Kybertest.cz," říká Monika Zahálková, výkonná ředitelka České bankovní asociace. Celkem 58 procent lidí si myslí, že se školy zabývají financemi ve svých vzdělávacích plánech málo nebo vůbec. Téměř třetina (32 procent) je přesvědčena, že samotní učitelé nejsou dost dobře proškolení ve finančních otázkách a víc než polovina (54 procent) se pak domnívá, že jsou děti ohledně povědomí o financích nedostatečně vedeny v rodině. Z průzkumu přitom vyplývá, že na finančním vzdělávání by se měl podílet hlavně stát. Myslí si to víc než dvě třetiny dotázaných (70 procent). S velkým odstupem je pak druhá v pořadí rodina, od které to čeká 30 procent dotázaných. Čtvrtina z nich pak tuto roli očekává od komerčních bank a pětina od České národní banky a Ministerstva financí.

Pomoc a rady v oblasti peněz a finančních produktů častěji vyhledávají lidé s nižším vzděláním. Více než desetina dotázaných (13 procent) tvrdí, že si v této oblasti vždy vystačí se svými znalostmi. Celkem 60 procent pak uvedlo, že si většinou vystačí, ale v některých případech se raději poradí s odborníkem. Často si s financemi neví rady víc než pětina respondentů a vůbec se pak v této oblasti nevyzná 6 procent lidí.

(RED)

48. Mastercard posiluje aktivity v oblasti kyberbezpečnosti. Bude simulovat a vyhodnocovat útoky

Tisk ● Bankovnictví - příloha; str. 10, 11 (Ekonomika / Finance / Právo) ● 14. 9. 2022

Vydavatel: **4H production s.r.o. (cz-28471831)** ● Rubrika: **Kyberbezpečnost**

Dosah: 12 248 ● GRP: 0.14 ● OTS: 0.00 ● AVE: 138000.00 Kč

Odkaz: náhled

Kyberbezpečnost

Mastercard posiluje aktivity v oblasti kyberbezpečnosti. Bude simulovat a vyhodnocovat útoky

Odborníci očekávají, že roční výše škod způsobovaných kyberkriminalitou dosáhne do roku 2025 v globálním měřítku hodnoty 10,5 bilionu amerických dolarů. Inovace v oblasti kyberzabezpečení mají proto pro obory, ve kterých probíhá překotná digitalizace, zcela zásadní význam. Díky strategické investici do menšinového podílu ve firmě Picus Security může společnost Mastercard oznámit spuštění nové platformy Cyber Front, jejímž účelem je simulace a vyhodnocování útoků.

Nový nástroj bude sloužit firmám a státním úřadům k posilování provozní odolnosti vůči kybernetickým útokům. Využívání nové platformy je součástí rozrůstající se poradenské činnosti společnosti Mastercard v oblasti kyberbezpečnosti a řízení rizik.

Platforma Cyber Front, která funguje v nepřetržitém režimu, pomáhá klientům posilovat jejich digitální ekosystémy ověřováním účinnosti dílčích systémů zabezpečení v prevenci a detekci kybernetických hrozeb. Díky průběžně aktualizované knihovně, která obsahuje více než 3 500 scénářů reálných hrozeb, dokáže platforma Cyber Front odhalovat bezpečnostní nedostatky a poskytovat rady ohledně posílení zabezpečení v reálném čase. Zásluhou průběžného testování a ověřování mají organizace možnost své investice do kyberbezpečnosti nadále zlepšovat. Účelem platformy je poskytovat možnost kontroly, nakolik jsou stávající systémy zabezpečení účinné, a identifikovat oblasti vyžadující lepší ochranu, a to jak bezprostředně, tak v dlouhodobém horizontu.

„Našim klientům a partnerům pomáháme těžit z možností digitální transformace a současně čelit komplikacím, které jsou s ní spojené. S ohledem na stoupající výši škod plynoucích z narušení bezpečnosti dat je kyberbezpečnost v digitální transformaci jedním z nejvýznamnějších témat. Organizace dnes potřebují nejen mít dostatečně silnou ochranu, ale musí zároveň testovat, učit se a přizpůsobovat se nárokům zítřka. Investice společnosti Mastercard do firmy Picus Security a spuštění platformy Cyber Front umožní činit rychlejší a lépe informovaná kyberbezpečnostní rozhodnutí, z nichž budou mít prospěch nejen přímo naši partneři, ale také jejich zaměstnanci a klienti," uvedla ke spuštění platformy Raj Seshadri, prezidentka divize Data & Services společnosti Mastercard.

V oblasti investic do kyberbezpečnosti má Mastercard bohatou globální historii

Společnost Mastercard již realizovala celou řadu investic do nastupujících technologií v oblasti kyberbezpečnosti, které uživatelům poskytují

pohled na kybernetická rizika, jež je mohou ohrožovat jak směrem zvenku dovnitř, tak naopak. Průkopnická technologie nástroje RiskRecon, určená ke skenování a hodnocení rizik třetích stran směrem zvenku dovnitř, umožňuje klientům po celém světě posuzovat rizikovost jejich partnerů. Více než tisícovce klientů už pomáhá nástroj Cyber Quant,, aby mohli mít přehled o svých bezpečnostních rizicích ve směru zevnitř ven včetně schopnosti jejich kvantifikace ve finančním vyjádření. Společně umožňují obě řešení několikastupňový přístup ke zvládání rizik spolu s využíváním pokročilé umělé inteligence a proprietárních i veřejně přístupných dat.

Řešení Cyber Front dále rozšiřuje komplexní, na datech založené služby společnosti Mastercard, které firmám pomáhají dosahovat požadovaných výsledků a minimalizovat rizika. Mezi poskytované služby patří ověřování totožnosti, diagnostika podvodného jednání, poskytování informací o spotřebitelích a portfoliích či poradenské a marketingové služby. Nedávno zároveň poradenský tým společnosti Mastercard uzavřel partnerství s Obchodní komorou v Paříži, což dalo vzniknout osmnáctiměsíčnímu vzdělávacímu programu pro zhruba pět tisíc malých podniků. Program se zaměřuje na posilování kybernetické odolnosti a jeho účelem bude seznamovat účastníky s finančními dopady kybernetických rizik a poskytovat jim jasná doporučení a návody, jak minimalizovat vystavení se rizikům. Divize Cybersecurity & Risk Practice mimoto spolupracuje například i s největší finanční institucí v Guatemale, Banco Industrial. Díky této spolupráci přispívá divize k lepšímu poznání možných kybernetických rizik v rámci ekosystému firemních klientů instituce.

Všechny uvedené činnosti dokládají silné zaměření společnosti Mastercard na posilování ochrany proti kybernetickým hrozbám i upevňování znalostí v globálním měřítku. V prosinci 2021 podepsala společnost Mastercard partnerskou smlouvu s Europolem o sdílení informací, identifikaci významných činností a posilování kybernetické odolnosti v Evropě. Uzavření partnerství s Europolem následovalo po otevření Centra kybernetické odolnosti společnosti Mastercard v belgickém Waterloo. V kanadském Vancouveru zase Mastercard pokračuje v investicích do svého Globálního centra excelence pro informace a kyberbezpečnost, který se zaměřuje na urychlování inovací v oblasti digitalizace a kyberbezpečnosti, umělé inteligence a internetu věcí.

> Našim klientům a partnerům pomáháme těžit z možností digitální transformace a současně čelit komplikacím, které jsou s ní spojené.

Ryze pro české spotřebitele – #nePINdej!

Aktivity Mastercard v oblasti kyberbezpečnosti nejsou jen mezinárodního charakteru. Jednou z nejnovějších – ryze českých aktivit, kterou Mastercard podpořila – je i vzdělávací kampaň v oblasti kyberbezpečnosti, již představila Česká bankovní asociace (ČBA) s orgány státní správy a s klíčovými firmami českého byznysu #nePINdej! Má upozornit na sílící nebezpečí podvodů na internetu. Představí nejčastější kybernetické útoky a formou hravého testu na www.kybertest.cz naučí, jak jim nenaletět. Kampaní chce ČBA oslovit širokou veřejnost – mladistvé od dvanácti let, dospělé i seniory.

„Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobný než za celý loňský rok. Dramaticky přitom narostly zejména podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším. Zatímco před dvěma lety se jejich počet pohyboval v nízkých stovkách, letos mluvíme již o desítkách tisíc. A vzrostla i jejich úspěšnost. Téměř každý druhý podvodný telefonát v současné době bohužel končí škodou pro klienta. Průměrná částka, o kterou klienti při těchto útocích přijdou, je přitom dost vysoká, zhruba čtvrt milionu korun," uvedla Monika Zahálková, výkonná ředitelka České bankovní asociace.

Její slova potvrzuje i Lukáš Kintr, ředitel Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). „Žijeme v digitální době, která nám mnohé věci usnadňuje, ale také přináší spoustu rizik, mezi něž patří i rostoucí počet různých kyberútoků. Detekujeme vysoké počty nejen podvodných telefonátů, ale i textových zpráv či e-mailů, a nelze očekávat, že by se jejich míra měla snižovat. Nejlepší obranou proti těmto pokusům nadále zůstává obecná osvěta, tedy informovanost a poučenost veřejnosti, aby byli lidé schopni vishing a podobné snahy rozpoznat," upřesňuje Lukáš Kintr.

Samotný kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. „Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Totéž platí pro útoky hackerů – různé praktiky zkoušejí na mladší generaci, další na osoby středního věku a odlišně jednají s nejstaršími spoluobčany.

49. „Zablokujeme vám účet.“ Poslechněte si telefonát falešného bankéře s obětí

Online ● seznamzpravy.cz (Zprávy / Politika) ● 15. 9. 2022, 10:04

Vydavatel: **Seznam.cz, a.s. (cz-26168685)** ● Autor: **Petr Juna, Jiří Burýšek**

Dosah: 1 702 492 ● GRP: 18.92 ● OTS: 0.19 ● AVE: 79177.75 Kč ● Interakcí: 623

Odkaz: https://www.seznamzpravy.cz/clanek/fakta-zablokujeme-vam-ucet-poslechnete-si-telefonat-falesneho-bankere-s-obeti-214145

Podvodníci dokážou klientům bank na dálku vybrat celý účet. Ilustrační fotografie.

10:04

Psychologický nátlak domnělé autority a strach z toho, že člověk přijde o všechny peníze. Seznam Zprávy na unikátní reálné nahrávce ukazují, jak funguje podvod, který Čechy jen za poslední dva roky připravil o desítky milionů.

Představil se jako pracovník banky a ženě na druhé straně telefonu oznámil, že má napadený účet. Číslo, ze kterého volá, odpovídá – jde o její banku. Žena je opravdu obětí podvodu. Ale jiného, než by se mohlo zdát. Domnělý bankéř je totiž ve skutečnosti útočník, který začíná psychologickou hru, na jejímž konci zůstává napadenému prázdný účet.

Buď pošlete peníze, nebo zkonfiskujeme účet

Útočník vystupuje v roli autority, která má poškozené pomoci zachránit peníze. Jeho cílem je donutit oběť, aby šla na pobočku a tam si vybrala celý obsah svého účtu, nebo dokonce vzala úvěr, a pak peníze poslala jemu. Pro zloděje je přitom důležité, aby nikomu nevěřila. „Buď daná osoba vlastní duplikát vašeho občanského průkazu nebo došlo ke zneužití postavení nějakého bankéře z pobočky. Což by znamenalo, že vaše údaje zaprodal třetím stranám, nebo osobně zneužil," tvrdí podvodník.

Skutečný útočník se tak snaží o jediné: přesvědčit oběť, že se ji někdo – možná dokonce její bankéř – pokusil okrást. Tváří se proto jako zaměstnanec banky a přesně navádí oběť k tomu, jak mu má poslat peníze. To celé pod záminkou pomoci a ochrany klientky.

Jakmile podvodník zjišťuje, že jeho cíl nepostupuje podle scénáře, který se mu hodí, začíná být agresivnější. „Já vás tady nebudu nějakým způsobem přemlouvat," tlačí na ženu. „Váš účet bude tedy konfiskován po dobu vyšetřování. Takže já udělám celkovou blokaci účtu." Podvedená tak stojí před dilematem – uvěřit muži na telefonu, že její účet je opravdu ohrožený, nebo věřit své bankéřce?

Výše uvedené citace a situace jsou skutečné. Jde o část pokusu o podvod, který si nahrála klientka České spořitelny a banka ji poskytla Seznam Zprávám. Celý telefonát si můžete poslechnout níže. Hlasy obou stran jsou upravené.

Příběh, jehož část je zachycená na nahrávce, skončil dobře: žena nátlaku nepodlehla a šla si informaci ověřit na svoji pobočku.

Není ale ojedinělý. Se stejným podvodem se setkal třeba manažer jedné z brněnských poboček České spořitelny Brian Pašek, kterému se podařilo klientku před podvedením zachránit doslova na poslední chvíli. V momentě, kdy si vyřizovala úvěr.

„Přišla jedna z našich klientek, která požadovala hotovostní úvěr, přičemž po pár dalších dotazech znejistěla," popisuje. „Zeptal jsem se proto, jestli se nemůže jednat o podvod."

V tu chvíli se ukázalo, jak silně na ni útočník psychologicky působil. Žena nejdříve zapírala a říkala, že peníze opravdu potřebuje.

Bankéř se proto zeptal přímo a popsal, jakým způsobem mohou útočníci postupovat: „Váš účet byl napadený, je potřeba, abyste přišla na pobočku.“ Podvodníci jsou si přitom vědomi toho, že v menších městech jsou vztahy bankéřů s klienty užší. Podvedenou tak směřovali do Brna, kde ji nikdo neznal a také ona neznala nikoho. I proto zaměstnancům banky nevěřila ani poté, co jí podvod vysvětlili.

Vžili jsme se do role podvedeného

Redaktor Seznam Zpráv Petr Juna a youtuber Jiří Burýšek se nechali naoko podvést stále oblíbenějším trikem falešné investice. Podívejte se, jak celý podvod probíhá.

Nahrávka: pozor na podvodné telefonáty. Takhle vás okradou o tisíce

13. 9. 14:15

Když zaměstnanci získali její důvěru, rozplakala se. „V podstatě jí namluvili, že v tom jede i někdo zevnitř banky, a proto nám, pracovníkům banky, nesmí sdělit, že jí někdo volal, že je účet napadený,“ vzpomíná Pašek. Klientku pak uklidnil s tím, že žádný úvěr rozjednaný nemá a že o žádný žádat nemusí.

Bankéř si ale všiml, že žena zakrývá rukou mobilní telefon a telefonát s podvodníkem má dál aktivní. „S tím se setkáváme často. Jde o scénář, kdy oni poslouchají, co se na pobočce děje,“ vysvětluje Pašek. Důvod je prostý – útočníci pak lépe vědí, co podvedeným v bance říkají, a mohou se pokusit tuto obranu obejít.

Zaměstnanci banky proto ženu instruovali, co má podvodníkovi říkat, poté si telefon

Zaměstnanci banky proto ženu instruovali, co má podvodníkovi říkat, poté si telefon převzali a útočníka konfrontovali. Ten se ale dál vydával za zaměstnance a chtěl na telefon zpátky ženu, kterou se pokoušel podvést.

Když šla klientka ven, šel Pašek s ní. A zjistil, že útočník to stále nevzdal. „Řekl jí, že by měla jít na jinou pobočku, že účet byl napaden a podobně," popisuje bankéř.

Podle něj se snaží podvodníci v lidech co nejvíce udržovat nejistotu. I proto volali ženě dál a ptali se jí, proč úvěr nedostala. „Pak jí začali vyhrožovat zablokováním účtu, tvrdili, že se půl roku nedostane k penězům a podobně," popisuje Pašek stejnou formu nátlaku, jakou používal podvodník z nahrávky výše. Ani tady díky bankéřům trik zlodějům nevyšel.

Falešné dokumenty a desítky milionů za dva roky

Ne každý útok však má šťastný konec. „Zavolali paní, ne úplně seniorního věku, z Pardubic, nebo Hradce, která tomu uvěřila," vzpomíná na konkrétní podvod předseda Komise pro bankovní a finanční bezpečnost České bankovní asociace Petr Barák.

„Řekli jí, že peníze bude muset vložit do konkrétního bitcoinmatu (*bankomat mimo jiné uzpůsobený na převod klasické měny na bitcoin, pozn. red.*). Věděli, kde bydlí, tak jí řekli, ať jede, dejme tomu z Hradce do Pardubic. Tak se domluvila se synem, peníze vybrala a syn ji odvezl do Pardubic. Rozleželo se jim to v hlavě až poté, co peníze vložili do bitcoinmatu."

Tento příklad ukazuje, jak lidé mohou pod psychickým nátlakem uvěřit příběhům, ke kterým by jinak přistupovali obezřetněji, s nedůvěrou. Ani to, že žena vedle sebe měla třicetiletého syna, který celý podvod sledoval z pozice třetí osoby, nevedlo k tomu, že by trik odhalili.

„Aby útočníci podpořili svou legendu, zasílají přes aplikaci WhatsApp fotografii své fiktivní zaměstnanecké karty a různé dokumenty opatřené logem vaší banky," vysvětluje Ondřej Kapr z Úřadu služby kriminální policie a vyšetřování Policejního prezidia ČR.

+3

Takzvaní navolávači jsou podle Kapra Češi, kteří výborně ovládají bankovní terminologii a jsou velmi manipulativní. Callcentrum ale může být kdekoliv na světě. „V tomto případě hrozí pachateli až 10 let vězení odnětí svobody," upozorňuje kriminalista.

Česká spořitelna řeší podle mluvčího Filipa Hrubého měsíčně jednotky klientů napadených podobným způsobem. Podvod se ale často daří zastavit před tím, než se oběti stane skutečná škoda. „Intenzivně spolupracujeme s policií a poskytujeme jim plnou součinnost," dodává Hrubý.

„Případů telefonického podvodu s legendou bankéře jsme za poslední dva roky zaznamenali více než tisíc se škodou v řádech desítek milionů korun," upřesňuje Kapr.

Jak předcházet podvodům

Vzhledem k rostoucímu množství podobných podvodů se rozhodla Česká bankovní asociace zlepšit finanční gramotnost v České republice, aby podobným podvodům předešla.

Nedávno například spustila ve spolupráci s policií edukativní projekt nePINdej, který má problematiku přiblížit a naučit lidi, jak se nestát obětí.

Součástí projektu je také online hra kybertest, kde si mohou lidé vyzkoušet, jestli by se na podvod nachytali.

Připravujeme: V dalším díle minisérie mapující bankovní podvody po internetu přinesou Seznam Zprávy rozhovor s policejním specialistou a expertem na finanční gramotnost z České bankovní asociace na téma jak se podvodníkům bránit.

50. Experti radí, jak nenaletět na rafinovanou hru podvodníků

Online ● seznamzpravy.cz (Zprávy / Politika) ● 16. 9. 2022, 14:40

Vydavatel: **Seznam.cz, a.s. (cz-26168685)** ● Autor: **Petr Juna**

Dosah: 1 702 492 ● GRP: 18.92 ● OTS: 0.19 ● AVE: 79177.75 Kč ● Interakcí: 49

Odkaz: https://www.seznamzpravy.cz/clanek/fakta-experti-radi-jak-nenaletet-na-rafinovanou-hru-podvodniku-214275

Online podvodníci připraví obyvatele Česka ročně o miliony korun.

14:40

Podvody v online prostředí zažívají v poslední době obrovský boom. Seznam Zprávy proto oslovily odborníky, aby se podělili o příběhy, zkušenosti, ale i tipy, jak se podvodníkům bránit.

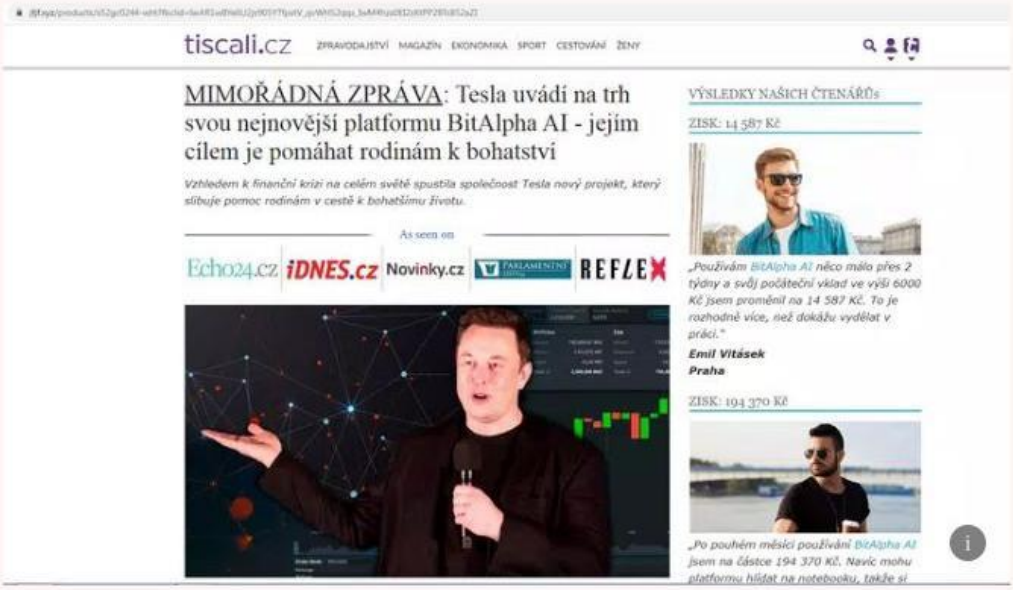
Prostřednictvím telefonu a počítače připraví podvodníci obyvatele Česka o miliony korun ročně. Seznam Zprávy v minulých dnech přinesly autentické nahrávky, které jejich metody názorně ukazují.

Připravit návod, který zaručeně ochrání každého, není v lidských silách. Redakce se o to pokusila alespoň částečně a spojila se proto s podplukovníkem Ondřejem Kaprem z Úřadu služby kriminální policie a vyšetřování Policejního prezidia ČR a předsedou Komise pro bankovní a finanční bezpečnost České bankovní asociace (ČBA) Petrem Barákem. Oba odborníci popsali své zkušenosti s tímto typem podvodů a dávají tipy, na co si dávat pozor.

Staronový hit: Falešná investice

„Podvody v online prostředí jsou na obrovském vzestupu. Je to trend současné doby," potvrzuje kriminalista. „Jedním z nejčastějších principů jsou podvody založené na možnosti investovat. Podvodníkům jde o to, aby lidé na něco klikli a nějakým způsobem investovali."

V obětech se snaží vyvolat důvěru odkazem na známé osobnosti, jejichž jména zneužívají ve fiktivních novinových článcích, na banky nebo třeba velké společnosti. V momentě, kdy nabídka člověka zaujme a on na ni klikne, mají podvodníci zpola vyhráno.



Ukázka falešného novinového článku.

„Jakmile útočník oběť kontaktuje, je těžké odolat. Je to velká psychologická hra, na kterou se bohužel nechá nachytat stále větší množství lidí a škoda bývá vysoká," vysvětluje Kapr. „Podvodníci využívají celou paletu prvků sociálního inženýrství, kterým vévodí důraz na přirozenou lidskou vlastnost, kterou je ziskuchtivost."

Poté, co podvodník oběti zavolá, chce po ní zaplatit vstupní investici do příslušné platformy, jejíž hodnota se obvykle pohybuje mezi 5 a 6 tisíci. Podvodníci jsou ale podle policejního rady velmi zkušení v sociálním inženýrství a jejich cílem nejsou nízké tisíce. „Pachatelům jde hlavně o to, aby z vás vylákali další peníze. Statisíce až miliony," upozorňuje Kapr a dodává, že ani ukradené miliony nejsou nic neobvyklého.

Vžili jsme se do role podvedeného

Redaktor Seznam Zpráv Petr Juna a youtuber Jiří Burýšek se nechali naoko podvést stále oblíbenějším trikem falešné investice. Podívejte se, jak celý podvod probíhá.

Nahrávka: pozor na podvodné telefonáty. Takhle vás okradou o tisíce

13. 9. 14:15

Dalším krokem podvodníků u falešné investice proto bývá pokus o vzdálené připojení do počítače oběti. „Buď se dívají, jestli tam máte ještě další peníze," vysvětluje Petr Barák z ČBA, „což znamená, jde mu o to ještě něco získat." Jakkoliv to zní hrozivě, tato varianta je ten lepší scénář. „Pak je ještě varianta, že jakmile se na účet dostanou, chtějí ho mít pod svým vlivem. Aby klient nevěděl, co se s účtem děje," vysvětluje odborník.

Banka pošle oběti potvrzující zprávu a podvodníci ji přesvědčí, aby krok autorizovala. Netuší přitom, že potvrdila spárování mobilního zařízení útočníka jako autorizační prvek. Podvodníci poté například zkoušejí, zda se jim povede vzít si na jméno oběti půjčku nebo kontokorent. I proto podle ČBA narůstají škody na jednoho podvedeného průměrně do stovek tisíců korun.

Jak přitom Barák zdůrazňuje, neexistuje scénář, při kterém by se bankéř připojoval na dálku do klientova počítače.

Oba experti se shodují, že lidé často ani nevědí, že jsou podvedeni. Zjistí to až v momentě, kdy se pokusí peníze z platformy vybrat. „Jsou známy případy, kdy klient má pocit, že peníze se zhodnocují. Vidí grafy, jak to roste. Až v okamžiku, kdy požádá o výběr, zjistí, že není co. Že peníze dávno nemá," vysvětluje Barák.

Člověk ale může přijít ještě o další prostředky. „Oni jsou dokonce tak drzí, že řeknou: ‚Ano, my vám to vyplatíme, ale protože to je předčasný výběr, musíte zaplatit poplatek za

zrušení.‘ Dál z nich tahají peníze,“ popisuje odborník. „Vytvářejí výmluvy, jako že peníze jsou zablokované a je potřeba něco dalšího zaplatit, nebo že jsou zadržené státním orgánem, který prověřuje jejich legálnost.“

Typické scénáře podle Petra Baráka

Vaše peníze jsou v ohrožení = Podvodník se vydává za pracovníka banky. Vyvolá strach na straně klienta tím, že mu tvrdí, že jeho peníze na účtu jsou v ohrožení a pokud je chce zachránit, je tady od toho, aby mu s tím pomohl, a je třeba jednat okamžitě.

Vaše peníze znehodnocuje inflace = Podvodník se vydává za investičního poradce banky / investiční společnosti. Nabízí buď jedinečnou možnost investovat a zhodnotit prostředky na účtu klienta, nebo sděluje klientovi, že se jeho předchozí investice, o které si navíc již sám klient myslel, že mu nic nevydělala, nečekaně zhodnotila a domlouvá s ním způsob jejího vyplacení. Pokud tomu klient uvěří, o své peníze přijde, a to i v druhém případě, kdy je výplata zhodnocené investice podmíněna úhradou nutných poplatků.

Snadný výdělek = Klient banky je vmanipulován do role takzvaného „bílého koně“, a to jako osoba, která za úplatu propůjčí svůj účet podvodníkům, kteří přes něj pak legalizují své příjmy z podvodů. Posílají si na takovýto účet odcizené peníze jiných klientů a jeho majitelem si je pak nechávají vybírat v hotovosti a vkládat například do bitcoinmatů – nakupují přes ně různé kryptoměny – nebo si nechávají posílat odcizené prostředky na jiné účty.

Bazarový prodej = Poté, co klient vystaví na některém bazarovém portálu svůj inzerát na prodej zboží, se mu obratem ozve na jeho telefon pachatel v roli zájemce o koupi zboží s tím, že požaduje umožnění úhrady prostřednictvím takzvané „bezpečné platby“.

Klient je nasměrován na falešné webové stránky, kde jsou od něj vyžadovány údaje k jeho platební kartě, a to včetně uvedení bezpečnostních prvků platební karty. Pokud klient toto vše vyplní, pachatelé ihned zadávají odchozí platby z jeho účtu s tím, že žádají od klienta pod záminkou, že mu již posílají peníze za zboží, aby jim tyto ve skutečnosti odchozí platby ze svého účtu potvrdil. Pokud klient nečte SMS autorizační zprávy ze své banky a jen potvrzuje to, co mu pachatelé říkají, autorizuje si tím sám podvodné platby a přichází o peníze.

Romance fraud = Nabídky na seznámení se s „důstojníkem US armády, lékařem v Africe, atraktivní dívkou ze zahraničí…“, kde je cílem z klienta vylákat postupně stále více peněz za různé

nutné výdaje (celní poplatky, poplatky za letenku, poplatky za vyvázání se z vykonávané činnosti a podobně). Pokud tomu poblouzněný klient/klientka věří a platí, přichází o peníze.

Existuje bohužel velké množství osamělých lidí, kteří ani po upozornění bank, že se jedná o podvod (banka například již zná účet příjemce z minulosti a již ví, že je spojen s tímto typem podvodů), nedbají a peníze odešlou. Případně pokud banka sama peníze odmítne odeslat, jsou schopni si je převést na účet v jiné bance a odeslat je odtud, kde jim je banka ještě sama neodmítne odeslat.

Jako obranu před ztrátou peněz doporučuje kriminalista Kapr hlavně neinvestovat na platformách, které nejsou ověřené. Zároveň však zdůrazňuje, že není dobré spoléhat se jen na online recenze, které se dají zfalšovat.

„Nenechte se zlákat lacinou reklamou, falešnými recenzemi a slibem zaručeného zisku, který je bez rizika," radí. „Investování je vždy riziková záležitost a každý nese sám odpovědnost za své kroky. Navíc v těchto případech vlastně nejde ani o investici, protože peníze posíláte přímo na účet ovládaný pachatelem nebo si je prostě podvodník převede sám."

Ondřej Kapr také varuje před přehnanou důvěrou ve své schopnosti. „Četl jsem studii, že těmto podvodům často naletí člověk, který je vzdělanější, inteligentnější," upozorňuje. „Jde o to, že víc důvěřuje svojí intuici. Naopak člověk, který v životě zažil zklamání, si může říct, že by zase naletěl."

Není bankéř jako bankéř

Dalším aktuálním hitem mezi podvodníky je telefonát, ve kterém se oběť dozvídá, že její účet byl napaden a že má peníze převést jinam.

Telefonní číslo skutečně odpovídá tomu, které banka používá. Útočníci posílají i oficiálně vypadající dokumenty, aby zvýšili svou důvěryhodnost. S použitím těchto nástrojů pak manipulují oběti, aby jim pod silným psychickým tlakem sama peníze dobrovolně poslala

manipulují oběti, aby jim pod silným psychickým tlakem sama peníze dobrovolně poslala.

„Mají hlavičkový papír dané banky a mají napsáno, že jde o bezpečný účet pro ochranu peněz," popisuje Barák. „Je to vytvořené jen proto, aby to vzbudilo dojem, že je všechno v pořádku."

Jakmile ale člověk peníze pošle, může se s nimi rozloučit.

Jinou variantou stejného podvodu je, že podvodníci donutí oběť vybrat všechny své prostředky a pošlou jí adresu bitcoinového bankomatu, kam má finance vložit. Barák se tak v praxi setkává s až neuvěřitelnými příběhy. „Zavolali paní, ne úplně seniorního věku, z Pardubic, nebo Hradce, která tomu uvěřila," vzpomíná na konkrétní podvod. „Řekli jí, že peníze bude muset vložit do konkrétního bitcoinmatu. Věděli, kde bydlí, tak jí řekli, ať jede, dejme tomu, z Hradce do Pardubic. Tak se domluvila se synem, peníze vybrala a syn ji odvezl do Pardubic. Rozleželo se jim to v hlavě až poté, co peníze vložili do bitcoinmatu."

Autentická nahrávka: Jak probíhá podvod

Psychický nátlak, vyhrožování i falešná nabídka pomoci. Poslechněte si, co všechno zažívají oběti vishingu.

Pozor na tento telefonát. Podvod, který připravil Čechy o desítky milionů

VČERA 10:04

U tohoto typu podvodu je ideální pamatovat na to, že postup, který praktikují podvodníci, by skutečná policie ani banka nezvolily. Všechno je navíc možné řešit i osobně, takže před

jakýmkoliv zásadnějším krokem je dobré jít na pobočku banky nebo policie a zeptat se, jestli se nejedná o podvod.

Útoků přibývá, banky sází na prevenci

Útoků v kyberprostoru výrazně přibývá. Podle České bankovní asociace se devět z deseti organizací dotázaných Národním úřadem pro kybernetickou bezpečnost v roce 2021 setkalo s phishingovým útokem nebo pokusem o něj. Pokus o útok zaznamenalo také 81 % bankovních institucí. Počet útoků na klienty bank se pak za dva roky zečtyřnásobil.

Banky se proto ve spolupráci s policií rozhodly ještě více zaměřit na prevenci. Jako příklad může sloužit nedávno spuštěný edukativní projekt nePINdej, který má problematiku přiblížit a naučit lidi, jak se nestat obětí podvodu. Součástí toho je například online hra kybertest, kde si mohou lidé vyzkoušet, jestli by před útočníky obstáli.

Více o kyberútocích na klienty bank

Detailně se kyberútokům v bankovnictví věnovaly Seznam Zprávy například v tomto článku:

Kyberútoků na banky a jejich klienty přibývá. Jaké jsou typické scénáře
6. 9. 18:33

Podle Lukáše Kropíka z České spořitelny existuje několik rad, které je dobré si pamatovat. Například jde o kontrolu telefonního čísla, ze kterého někdo volá. Není to sice stoprocentní zbraň, ale na internetu je možné dohledat, jestli s volajícím měl někdy někdo v minulosti negativní zkušenost.

„Nikdy do telefonu nesdělujte citlivé a bezpečnostní údaje, jako jsou třeba bezpečnostní údaje k internetovému bankovnictví (vaše ID a heslo, datum narození) nebo ke

údaje k internetovému bankovnictví (vaše ID a heslo, datum narození) nebo ke kartám (číslo karty, platnost karty, PIN, třímístný kód CVV/CVC z její zadní strany),“ vypočítává dále Kropík. „Chráníte tím především své peníze.“

Upozorňuje také na to, že člověk by nikdy neměl předávat bezpečnostní kód z SMS a v rámci dvoufaktorového ověření neměl potvrzovat něco, co nedělá on sám.

„Některé banky již nyní pracují na možnosti ověření, zda vám skutečně volá zaměstnanec banky,“ vysvětluje Kropík. „Například Česká spořitelna během podzimu umožní v bezpečností aplikaci George klíč u všech příchozích hovorů z banky jednoduše ověřit, zda volá skutečný bankéř. Již od jara letošního roku tuto funkcionalitu testuje na vybraných call centrech.“

51. #nePINdej!

Online ● pribramsko.eu (Regionální zprávy) ● 20. 9. 2022, 10:41

Dosah: 739 ● GRP: 0.01 ● OTS: 0.00 ● AVE: 4577.33 Kč

Odkaz: https://pribramsko.eu/nepindej-12254

www.turistika-brdy.cz | www.ohkpb.cz | www.kdno.cz |

Příbramsko.eu

Server www.pribramsko.eu byl založen 13. května 2008

Dobré dopoledne, je úterý 20.9.2022, 10:49. Dnes má sv

Zprávy | Hydepark | Kultura a sport | Zdravý životní styl | Historie | Kontakty

#nePINdej!

2022-09-20 10:16:13 | PČR, por. Bc. Monika Schindlová, DiS. ©

Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Jak vyplývá z dat České bankovní asociace, na jednoho poškozeného klienta připadá průměrná škoda ve výši 161 tisíc korun. U vishingu, neboli případů podvodného navolávání, jsou částky až čtvrtmilionové.

(Ilustrační foto archiv)

Klíčovým prvkem kampaně s názvem **#nePINdej!** je interaktivní vzdělávací www.kybertest.cz, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět.

Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. V kybertestu jsou simulovány podvodné SMS, zobrazovací okna k připojení k WIFI sítím, phishingové emaily, zvukové nahrávky podvodných telefonů a mnohé další, tak, aby si je každý uživatel moderních technologií mohl bezpečně vyzkoušet. Testové otázky byly připravovány odborníky na základě reálných případů, jimiž se podvodníci snaží své oběti nachytat.

Pachatelé se při útocích snaží překonávat zejména lidský faktor a pod nejrůznějšími legendami využívají nátlaku, strachu a časové tísně pro záchranu peněz nebo pro realizaci finanční transakce. Mezi nejčastější podvodné legendy patří:

Podvodné navolávání:

Pachatelé se vydávají například za bankéře, policisty, pracovníky technické podpory a snaží se z lidí pod vlivem strachu vylákat peníze, nebo vzdálený přístup do zařízení oběti, který následně zneužije.

Nabídka výhodných investic:

Přesvědčivá lákavá reklama a manipulativní jednání. Cílem pachatele je vylákat z oběti co možná nejvíce finančních prostředků a využívá k tomu přirozenou ziskuchtivost každého z nás.

Reverzní inzertní podvody:

Pachatel zareaguje na váš inzerát. Podstrčí vám fiktivní platební bránu, kde vyplníte citlivé bankovní údaje a místo peněz za inzerované zboží přicházíte o všechny úspory.

Podvody typu Nigerijské dopisy:

Princip, který funguje už více jak sto let. Pachatelé sázejí na kvantitu. Vždy se najde někdo, kdo se nechá nachytat na slibovanou cennou zásilku nebo domnělou pomoc. Často zde hraje velkou roli láska.

Klasické podvody typu phishing a smishing:

Stále dokonalejší a složitě rozpoznatelné podvodné emaily a SMS nabídky. Na první pohled již nenajdeme podezřelé znaky.

https://www.policie.cz/clanek/nepindej.aspx

PČR, por. Bc. Monika Schindlová, DiS. ©

52. Policie varuje před bankovními podvody. Jejich počet se v posledních letech zvýšil

Online ● zpravypribram.cz (Regionální zprávy) ● 21. 9. 2022, 13:00

Rubrika: **Krimi**

Dosah: 255 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 2466.00 Kč

Odkaz: https://www.zpravypribram.cz/policie-varuje-pred-bankovnimi-podvody-jejich-pocet-se-v-poslednich-letech-zvysil/

ČR – Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Jak vyplývá z dat České bankovní asociace, na jednoho poškozeného klienta připadá průměrná škoda ve výši 161 tisíc korun. U vishingu, neboli případů podvodného navolávání, jsou částky až čtvrtmilionové.

Klíčovým prvkem kampaně s názvem **#nePINdej!** je interaktivní vzdělávací www.kybertest.cz, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim nenaletět. Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. V kybertestu jsou simulovány podvodné SMS, zobrazovací okna k připojení k WIFI sítím, phishingové emaily, zvukové nahrávky podvodných telefonů a mnohé další, tak, aby si je každý uživatel moderních technologií mohl bezpečně vyzkoušet. Testové otázky byly připravovány odborníky na základě reálných případů, jimiž se podvodníci snaží své oběti nachytat.

Pachatelé se při útocích snaží překonávat zejména lidský faktor a pod nejrůznějšími legendami využívají nátlaku, strachu a časové tísně pro záchranu peněz nebo pro realizaci finanční transakce. Mezi nejčastější podvodné legendy patří:

Podvodné navolávání:
Pachatelé se vydávají například za bankéře, policisty, pracovníky technické podpory a snaží se z lidí pod vlivem strachu vylákat peníze, nebo vzdálený přístup do zařízení oběti, který následně zneužije.

Nabídka výhodných investic:
Přesvědčivá lákavá reklama a manipulativní jednání. Cílem pachatele je vylákat z oběti co možná nejvíce finančních prostředků a využívá k tomu přirozenou ziskuchtivost každého z nás.

Reverzní inzertní podvody:
Pachatel zareaguje na váš inzerát. Podstrčí vám fiktivní platební bránu, kde vyplníte citlivé bankovní údaje a místo peněz za inzerované zboží přicházíte o všechny úspory.

Podvody typu Nigerijské dopisy:
Princip, který funguje už více jak sto let. Pachatelé sázejí na kvantitu. Vždy se najde někdo, kdo se nechá nachytat na slibovanou cennou zásilku nebo domnělou pomoc. Často zde hraje velkou roli láska.

Klasické podvody typu phishing a smishing:
Stále dokonalejší a složitě rozpoznatelné podvodné emaily a SMS nabídky. Na první pohled již nenajdeme podezřelé znaky.

53. Kyber kampaň #nePINdej!

Online ● policie.cz (Jiné) ● 23. 9. 2022, 7:08

Dosah: 20 667 ● GRP: 0.23 ● OTS: 0.00 ● AVE: 19996.45 Kč

Odkaz: https://www.policie.cz/clanek/kyber-kampan-nepindej.aspx

ZPRAVODAJSTVÍ

Úvodní strana / Útvary Policie ČR / Krajská ředi

Policie České republiky – KŘP Karlovarského kraje

Kyber kampaň #nePINdej!

KARLOVARSKÝ KRAJ – Upozorňuje na nebezpečí podvodů na internetu.

Police České republiky se od začátku září 2022 připojila k rozsáhlé vzdělávací kampani České bankovní asociace a dalších partnerů, která upozorňuje na sílící nebezpečí podvodů na internetu.

Mezi nejčastější typy podvodů na internetu patří např. podvodné e-maily tzv. phising. Cílem těchto útoků je buď od Vás získat Vaše citlivé údaje jako např. číslo platební karty nebo Vás donutit k nechtěnému stažení škodlivého softwaru. Přibývá také podvodných SMS tzv. smishing. Velmi často se jedná o zprávy, které vypadají, jako by je zaslala některá z doručovacích společností či Vaše banka. Lákat Vás můžou také na vyzvednutí výhry apod. Všechny tyto SMS mají opět jediný cíl – vylákat z Vás citlivé údaje. Další způsob jak z Vás vylákat citlivé údaje nebo Vás připravit o peníze jsou podvodné telefonáty údajných bankéřů, policistů či investičních poradců tzv. vishing. Tento způsob je o to zákeřnější, neboť se jedná o telefonní hovor s „živým" člověkem, který chce svou oběť vystrašit a zároveň vzbudit důvěru, že je tím, kdo Vám pomůže. S Vámi získanou důvěrou Vás pak bude bude nutit k okamžité reakci a bude po Vás chtít přihlašovací údaje, údaje z platební karty aj.

Podvodů na internetu existuje celá řada. Kybernetičtí zločinci se při pokusech Vás okrást neustále zdokonalují. Jejich metody jsou dnes daleko sofistikovanější a kombinují nedostatečné zabezpečení Vašich chytrých telefonů a PC, znalost Vašich osobních dat, umění manipulace a moment překvapení.

Základní rady, jak "nenaletět":

- Poznejte svého nepřítele. Seznamujte se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenechte od pachatele do ničeho tlačit a vše si pečlivě promyslete.
- Jakmile je zpráva, e-mail, SMS, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamyslete nad tím, kam vypisujete citlivé údaje, nebo přeposíláte peníze.
- Když si nejste absolutně jistý, tak vždy raději vše ověřte jinou cestou.
- Pamatujte si, že pachatel dokáže napodobit jakékoliv telefonní číslo, či e-mailovou adresu.
- Nikdy neumožňujte vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřujete.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z Vaší platební karty.

Preventisté Krajského ředitelství policie Karlovarského kraje v rámci této kyber kampaně navštívili několik restauračních zařízení po celém Karlovarském kraji, kde rozdávali papírové prostírání z informacemi ohledně této kampaně. Součástí prostírání je i QR kód, který Vás odkáže na stránky www.kybertest.cz. Zde můžete vyzkoušet test, který představuje běžné situace, do kterých se můžete dostat a v nichž se Vás hackeři mohou snažit okrást. V kybertestu se dozvíte, jak útoky podvodníků rozpoznat a jak jim nenaletět. Popsány jsou zde podrobně také typy podvodů.

Jak už název sám napovídá, PIN nikdy nedej!

kpt. Bc. Zuzana Týřová
23. 9. 2022

#nePINdej kyber kampaň

Detailní náhled

#nePINdej kyber kampaň

Detailní náhled

#nePINdej kyber kampaň

Detailní náhled

#nePINdej kyber kampaň

Detailní náhled

E-mailem Vytisknout

54. V Karlovarském kraji byla zahájena preventivní kampaň #nePINdej!

Online ● nasregion.cz (Regionální zprávy) ● 26. 9. 2022, 12:35

Vydavatel: **A 11 s.r.o. (cz-27120805)**

Dosah: 44 364 ● GRP: 0.49 ● OTS: 0.00 ● AVE: 34914.53 Kč ● Interakcí: 1

Odkaz: https://nasregion.cz/v-karlovarskem-kraji-byla-zahajena-preventivni-kampan-nepindej-296899/

NÁŠ REGION

VYBRAT REGION

V Karlovarském kraji byla zahájena preventivní kampaň #nePINdej!

26.9.2022 Roman Kořínek

Karlovarští policejní preventisté v rámci kyber kampaně navštívili několik restauračních zařízení po celém Karlovarském kraji, kde rozdávali papírové prostírání s informacemi ohledně této kampaně. Zdroj: pčr

Karlovarští policisté se od začátku září 2022 připojují k rozsáhlé vzdělávací kampani České bankovní asociace a dalších partnerů, která upozorňuje na sílící nebezpečí podvodů na internetu. Mezi nejčastější typy podvodů na internetu patří podle policejní mluvčí Zuzany Týřové podvodné e-maily takzvaný phising.

„Cílem těchto útoků je buď od lidí získat citlivé údaje jako například číslo platební karty nebo je donutit k nechtěnému stažení škodlivého softwaru. Přibývá také podvodných SMS takzvaných smishing. Velmi často se jedná o zprávy, které vypadají, jako by je zaslala některá z doručovacích společností či banka," vysvětluje policejní mluvčí.

Pachatelé mohou lákat také například na vyzvednutí výhry. Všechny tyto SMS mají opět jediný cíl – vylákat z lidí citlivé údaje. Další způsob jak vylákat citlivé údaje nebo připravit důvěřivé lidi o peníze jsou podvodné telefonáty údajných bankéřů, policistů či investičních poradců takzvaný vishing.

„Tento způsob je o to zákeřnější, neboť se jedná o telefonní hovor s „živým" člověkem, který chce svou oběť vystrašit a zároveň vzbudit důvěru, že je tím, kdo mu pomůže. Se získanou důvěrou pak bude nutit k okamžité reakci a bude po chtít přihlašovací údaje, údaje z platební karty a tak dále. Podvodů na internetu existuje celá řada. Kybernetičtí zločinci se při pokusech okrást oběť neustále zdokonalují. Jejich metody jsou dnes daleko sofistikovanější a kombinují nedostatečné zabezpečení chytrých telefonů a PC, znalost osobních dat, umění manipulace a moment překvapení," doplňuje Zuzana Týřová.

Policisté proto připravili několik rad, jak se mají lidé, kteří se stanou obětí kyber šikany chovat a jak takzvaně nenaletět.

- Poznejte svého nepřítele. Seznamujte se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenechte od pachatele do ničeho tlačit a vše si pečlivě promyslete.
- Jakmile je zpráva, e-mail, SMS, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamyslete nad tím, kam vypisujete citlivé údaje, nebo přeposíláte peníze.
- Když si nejste absolutně jistý, tak vždy raději vše ověřte jinou cestou.
- Pamatujte si, že pachatel dokáže napodobit jakékoliv telefonní číslo, či e-mailovou adresu.
- Nikdy neumožňujte vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřujete.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z Vaší platební karty.

Preventisté Krajského ředitelství policie Karlovarského kraje v rámci této kyber kampaně navštívili několik restauračních zařízení po celém Karlovarském kraji, kde rozdávali papírové prostírání s informacemi ohledně této kampaně.

„Součástí prostírání je i QR kód, který odkáže na stránky www.kybertest.cz. Zde lidé mohou vyzkoušet test, který představuje běžné situace, do kterých se mohou dostat a v nichž se je hackeři mohou snažit

okrást. V kybertestu se dozví, jak útoky podvodníků rozpoznat a jak jim nenaletět. Popsány jsou zde podrobně také typy podvodů," dodala policejní mluvčí s tím, že hlavní sdělení kampaně, jak už název sám napovídá, PIN nikdy nedej!

Zdroj: vz/pčr

TÉMATA: #POLICIE #PREVENCE

55. Kybernetických útoků dramaticky přibývá

Online ● radioblanik.cz (Zprávy / Politika) ● 27. 9. 2022, 9:39

Vydavatel: **MEDIA BOHEMIA a.s. (cz-26765586)**

Dosah: 4 204 ● GRP: 0.05 ● OTS: 0.00 ● AVE: 10711.67 Kč

Odkaz: https://radioblanik.cz/index.php/aktualne/kybernetickych-utoku-dramaticky-pribyva

KYBERNETICKÝCH ÚTOKŮ DRAMATICKY PŘIBÝVÁ

Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů. Vyplývá to z dat České bankovní asociace. Právě proto ČBA ve spolupráci s orgány státní správy a s dalšími firmami spustila celonárodní vzdělávací kampaň **#nePINdej!**

Klíčovým prvkem kampaně je kyber test. Ten obsahuje devět nejčastějších podvodů v online prostředí. Lidé se tak zábavnou formou mohou naučit, jak podvodníkům nenaletět. Cílem testu není člověka za každou cenu nachytat, ale ukázat mu, na co si má dát pozor. Po každé otázce následuje správné řešení. Otázky se generují na míru podle různých věkových kategorií.

www.nepindej.cz

www.kybertest.cz

56. Kampaň #nePINdej!

Online ● slovo.proglas.cz (Jiné) ● 28. 9. 2022, 13:20

Autor: **Pavel Smolek**

Dosah: 178 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 1982.04 Kč

Odkaz: https://slovo.proglas.cz/kultura-a-vzdelavani/dopoledne-s-proglasem/kampan-nepindej/

Kampaň #nePINdej!

28. září 2022 Dopoledne s Proglasem Autor: Pavel Smolek

Dovolím si tvrdit, že podvodníci jsou staří jako lidstvo samo. V dnešní době se stále více zaměřují na podvody, které probíhají prostřednictvím internetu, a cílí na internetové bankovnictví. Proto Česká bankovní asociace spustila kampaň s názvem #nePINdej! Cíle a průběh kampaně si v rámci našeho dopoledního vysílání představíme s bezpečnostním expertem České bankovní asociace **Petrem Barákem** ve čtvrtek **29. září 2022 od 9.00**.

Na koho internetové podvody cílí? Jak probíhají? S jakými typy podvodů se mohou lidé setkat? A se jim bránit? Nejen na tyto otázky se budeme našeho hosta ptát.

Česká bankovní asociace už nyní registruje, že letos došlo k dvojnásobnému počtu podvodů ve srovnání s celým loňským rokem. Průměrná škoda je asi 160 000 korun. Ale nejsou výjimkou škody, které přesahují 1 000 000 korun i více! Přitom internetová kriminalita už necílí jen na seniory, ale doslova na kohokoliv. A každý druhý útok bývá úspěšný. I proto Česká bankovní asociace spustila Kybertest 2022, který má co nejširší veřejnosti ukázat s jakými typy podvodů se mohou setkat.

Pokud si náš rozhovor nebudete moci vyslechnout ať už prostřednictvím našeho vysílání, nebo třeba z audioarchivu, určitě se na Kybertest 2022 podívejte a vyzkoušejte si ho. Možeme prozradit, že náš redaktor Pavel Smolek dosáhl úspěšnosti 77 %. Je to málo, nebo hodně? Určitě to není 100 %, takže by mohl být docela pravděpodobně někdy podveden. A nestačí si Kybertest vyzkoušet. Je potřeba před internetovou kriminalitou varovat co nejvíce lidí ve svém okolí.

Pořad v souvislostech

29. 9. 2022, 09:00
Kampaň #nePINdej!

Budeme vysílat

29. 9. 2022, 00:05
Svatý Václav včera a dnes

29. 9. 2022, 09:00
Kampaň #nePINdej!

30. 9. 2022, 00:05
Kampaň #nePINdej!

Vysílali jsme

28. 9. 2022, 00:05
O životě v Teologickém konvi…

27. 9. 2022, 09:00
O životě v Teologickém konvi…

27. 9. 2022, 00:05
Karel Novotný a Nové Adalbe…

Audioarchiv

57. ČD pro vás, číslo 10/2022; str. 56

Tisk ● ČD pro vás; str. 56 (Životní styl / Móda) ● 29. 9. 2022

Vydavatel: **České dráhy, a.s. (cz-70994226)**

Dosah: 1 000 000 ● GRP: 11.11 ● OTS: 0.11

Odkaz: náhled

58. Preventivní beseda v Ostré

Online ● policie.cz (Jiné) ● 30. 9. 2022, 13:36

Dosah: 20 667 ● GRP: 0.23 ● OTS: 0.00 ● AVE: 19996.45 Kč

Odkaz: https://www.policie.cz/clanek/preventivni-beseda-v-ostre.aspx

ZPRAVODAJSTVÍ

Úvodní strana / Útvary Policie ČR / Krajská ředitelství policie / Středočeský

Policie České republiky – KŘP Středočeského kraje

Preventivní beseda v Ostré

NYMBURSKO – Projekt SafetyDays Roadpol a informace ke kyberprostoru odprezentovali policisté z Územního odboru Nymburk.

V úterý 20. 9. 2022 bylo v budově obecního úřadu Ostrá uspořádáno setkání s občany na témata bezpečnost na silnici a bezpečnost v kyberprostoru. První téma bylo k projektu SafetyDays Roadpol, kde je cílem osvěta široké veřejnosti s apelem na nula úmrtí na silnicích. Letošní rok je projekt zaměřen především na cyklisty. Zúčastněné jsme upozornili na to, že k nulové úmrtnosti na silnici můžou přispět právě oni svou zodpovědností a používáním cyklistické helmy a předali jim několik bezpečnostních rad, jak se chovat v dopravě. Společně pak byly probrány různé situace v dopravě, které byly doplněny skutečnými vyšetřovanými případy z okresu Nymburk.
Druhou část setkání měl plně ve své kompetenci nymburský kriminalista por. Bc. Viktor Vokál. S občany komunikoval na téma bezpečně v kyberprostoru a upozorňoval na negativní vlivy tohoto prostředí. Společně prodiskutovali nejčastější problematiku podvodů na internetu - od podvodného inzerátu až po podvodné investování. Jednotlivé případy byly probrány tzv. „lidskou řečí" a tak nebyla nutná znalost IT prostředí. Preventivních rad, jak nenaletět podvodníkům zaznělo skutečně mnoho. Závěrem nechybělo zmínění odkazu na kybertest #nePINdej.

por. Bc. Petra Potočná
Územní odbor Nymburk
30. září 2022

por. Bc. Viktor Vokál

59. ČBA NEWS

Tisk ● ČBA News; str. 1 (Ekonomika / Finance / Právo) ● 4. 10. 2022

Autor: **Monika Zahálková**

Odkaz: náhled

20/2022 For English version please click here.

ČESKÁ BANKOVNÍ ASOCIACE / CZECH BANKING ASSOCIATION

NEWS

Milé kolegyně, milí kolegové,

události poslední doby vstoupily zásadním způsobem do našich každodenních životů. Jsem ale přesvědčena, že je důležité nenechat se válkou, energetickou krizí či ekonomickými problémy zcela pohltit a že je třeba vnímat život nejen s těmito vážnými problémy, ale také s každodenními běžnými radostmi i starostmi.
Česká bankovní asociace se v současné době soustředí zejména na projekt opatření na podporu ekonomiky, který by měl být alternativou k vládou zamýšlenému zavedení mimořádné daně. Nicméně, nemůžeme při tom zapomenout na „běžnou" agendu. Počátkem října proběhne shromáždění členských bank a stavebních spořitelen. Budeme hodnotit aktivity ČBA v letošním roce a diskutovat o strategii pro rok příští. Další mimořádně významnou „mírovou" aktivitou asociace je vzdělávání veřejnosti v oblasti financí a bezpečného nakládání s nimi.
Proto již od října opět startujeme velmi úspěšný projekt Bankéři do škol, o který je rok od roku stále větší zájem. Letos bude jeho součástí i kyberbezpečnostní téma, představíme www.kyberhra.cz, verzi kybertestu ušitou na míru žákům základních a středních škol.
Věřím, že časem se prostor pro tyto aktivity opět vrátí do normálu.

Přeji Vám barevný podzim!

Monika Zahálková, výkonná ředitelka

60. Bankéři vyráží do škol už podeváté

Tisk ● ČBA News; str. 6, 7 (Ekonomika / Finance / Právo) ● 4. 10. 2022

Bankéři vyráží do škol už podeváté

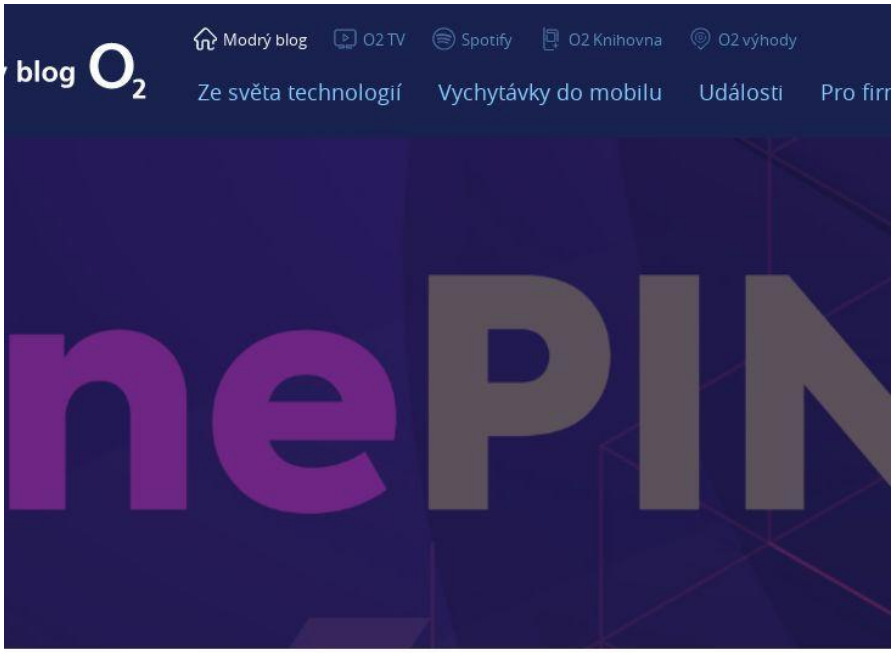
V říjnu a listopadu se odborníci z členských bank opět vydají přednášet v rámci projektu Bankéři do škol o základech finanční gramotnosti a kyberbezpečnosti. Tento finančně-vzdělávací projekt, který pořádá Česká bankovní asociace, má už devítiletou tradici a mezi školami je o něj čím dál tím větší zájem. Je určený žákům 8. a 9. tříd základních škol a studentům 1. a 2. ročníku středních škol a jeho cílem je rozvoj jejich základních znalostí z oblasti financí a kyberbezpečnosti. Součástí letošního ročníku je i speciální upravená verze interaktivního vzdělávacího kybertestu, kyberhra.cz, která je otázkami přizpůsobená této mladé generaci. Prostřednictvím Kyberhry se žáci a studenti mohou naučit rozpoznat kybernetické podvody a zjistit, jak se jim ubránit. Pokud chcete své děti v této oblasti také vzdělat, neváhejte Kyberhru společně s nimi vyzkoušet.

61. I vaše dítě může být cílem podvodníků. Poučte je o důležitosti kybernetické bezpečnosti! Pomůže Kyberhra

Online ● blog.o2.cz (Blogy) ● 4. 10. 2022, 8:55

Dosah: 205 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 2158.20 Kč

Odkaz: https://blog.o2.cz/2022/10/04/cil-podvodnik-dulezitost-kyberneticka-bezpecnost-kyberhra-pr1/



I vaše dítě může být cílem podvodníků. Poučte je o důležitosti kybernetické bezpečnosti! Pomůže Kyberhra

Dokáže vaše dítě rozeznat podvodné e-maily nebo SMS? A pokud ano, ví, jak při jejich obdržení správně postupovat? Kyberhra vyvinutá Českou bankovní asociací (ČBA) je to pomůže naučit.

Čím dál **mladší děti používají nejrůznější chytrá zařízení**. Ať už k výuce, ke hře nebo jako nástroj, jak zůstat ve spojení. Jen málo rodičů ale svého potomka poučí, na jaké nástrahy v kyberprostoru může narazit a jak se s nimi vypořádat.

I na kole se člověk musí nejdříve naučit jezdit

Jen základní nastavení nebo připojení k Wi-Fi dávno nestačí. Navíc **stále více dětí používá v mobilu i debetní karty a obsluhuje svůj účet**. Víte, na co si dát v kyberprostoru pozor?

Je toho hodně a je čím dál těžší podvody rozpoznat

Podvodníci jsou vynalézaví. Přichází se stále záludnějšími způsoby, jak se můžou dostat k citlivým údajům a zneužít je. Metody využívající sociálního inženýrství v emailové komunikaci tzv. **phishing**, podvodné SMS neboli **smishing** nebo dokonce podvodné telefonáty tzv. **vishing** jsou jen některými ze způsobů, jak se útočníci pokouší dostat k heslům, PINům nebo vás navést na odkaz se škodlivým malwarem.

Podvodníci se nevyhýbají ani sociálním sítím

Sociální sítě jsou pro mnoho dětí každodenní zábavou. Bohužel i tam se stávají snadným terčem nejrůznějších útoků a podvodů. Riziko navíc neustále narůstá. V letošním roce bylo zaznamenáno až **2x více podvodných útoků než v loňském, a to je teprve září**.

Prohlédnout léčku a nenechat se nachytat není jednoduché ani pro většinu dospělých. Jak si pak s takovými útoky mají poradit děti?

#nePINdej! a dokaž to

Spousta dětí, ale i dospělých, si často řekne**: „přeci nejsem naivní a podvod poznám" – je to ale skutečně tak?**

ČBA proto zahájila interaktivní vzdělávací kybertest v rámci edukativní kampaně **#nePINdej!**. Spolu se svými partnery, včetně společnosti O2, přinesla možnost, jak se formou hry naučit rozpoznávat podvodné maily, SMS, telefonáty, aplikace, nebo e-shopy, webové stránky či veřejné Wi-Fi sítě.

Zvládneš projít Kyberhrou?

Pro žáky druhého stupně základních škol a středoškoláky **ČBA** aktuálně přináší speciální upravenou verzi **www.kyberhra.cz**. Možná i vás překvapí, jak propracované triky podvodníci používají.

Neváhejte a **nechte děti vyzkoušet si vše na vlastní kůži** a objevit, jak podvody rozpoznat a účinně se jim bránit.

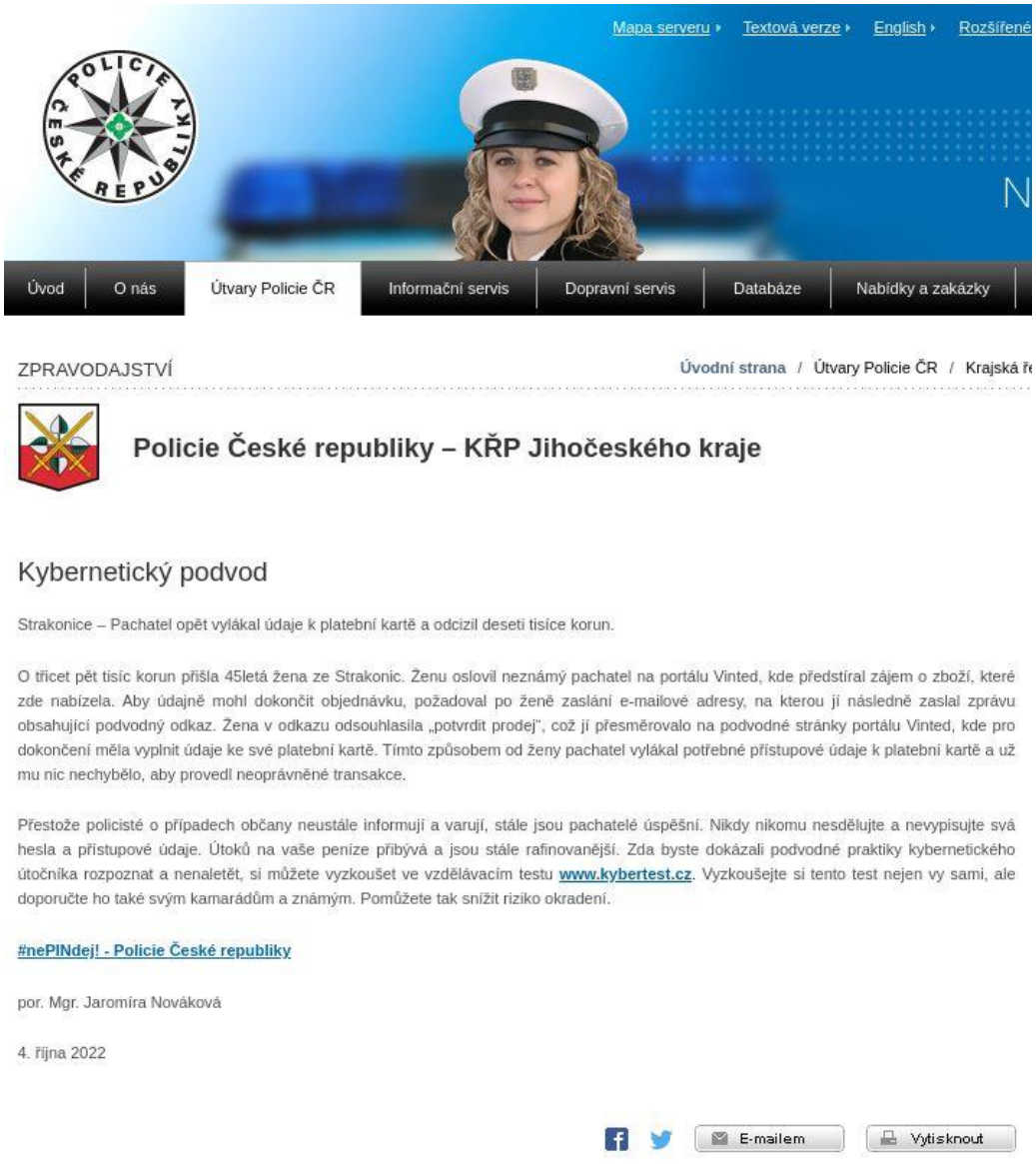
Ohodnoťte tento příspěvek!

62. Kybernetický podvod

Online ● policie.cz (Jiné) ● 4. 10. 2022, 9:16

Dosah: 20 667 ● GRP: 0.23 ● OTS: 0.00 ● AVE: 19996.45 Kč

Odkaz: https://www.policie.cz/clanek/kyberneticky-podvod.aspx



63. Podvody na internetových inzertních portálech

Online ● policie.cz (Jiné) ● 4. 10. 2022, 9:39

Dosah: 20 667 ● GRP: 0.23 ● OTS: 0.00 ● AVE: 19996.45 Kč

Odkaz: https://www.policie.cz/clanek/podvody-na-internetovych-inzertnich-portalech.aspx

ZPRAVODAJSTVÍ

Úvodní strana / Útvary Policie ČR / Krajská ředitelství policie / Středočesk

Policie České republiky – KŘP Středočeského kraje

Podvody na internetových inzertních portálech

PŘÍBRAMSKO - Říjen je měsícem kybernetické bezpečnosti.

Určitě je vhodné připomenout, jaká úskalí s sebou digitální prostředí přináší. Minulý týden přijali policisté na Příbramsku během čtyř dnů oznámení o pěti případech reverzních inzertních podvodů.

Většinou se jedná o podobný scénář. Pachatel zareaguje na váš inzerát. V oznámených případech šlo o prodej kopaček, oblečení, autobaterie, sedací soupravy a historických hrníčků. Falešný kupující předstírá zájem o prodávané zboží. Následně vám nabídne zajištění veškerého komfortu spojeného s přepravou i platbou a zašle vám fiktivní odkaz zpravidla na přepravní společnost. Pokud na něj prodávající klikne, je přesměrován na podvrženou platební bránu, kde pak vyplní citlivé bankovní údaje, údaje k platební kartě. Místo připsaných peněz z prodeje zboží ale poté zjistí, že mu naopak na účtu chybí část jeho úspor. V uvedených pěti případech se jednalo o částku téměř dvě stě tisíc korun.

Terčem útočníků jsou zejména prodávající, kteří si zvolili platební metodu – zasílání peněz z karty na kartu prostřednictvím peněženky zvoleného bazaru. Prodávající nepředpokládají, že se z nich snaží někdo získat přístupové údaje k účtům a do internetového bankovnictví. Mají zájem zboží prodat co nejdříve, a proto slepě spolupracují.

Jak se podvodníkům bránit? Důležité je vědět, že neklikám na odkazy do internetového bankovnictví obdržené v SMS zprávě či e-mailu. V žádném případě ani nepřeposílám autorizační kódy a za žádných okolností neposkytuji vzdálený přístup k počítači. Občané si také nyní mohou vyzkoušet interaktivní www.kybertest.cz, který je zábavnou formou seznámí s nejčastějšími kybernetickými podvody a naučí je, jak je rozpoznat a jak jim nenaletět.

To nevymažeš!
Dalším nebezpečím v digitálním prostředí je sexting. Jde o sdílení vlastních intimních fotografií či videí velmi často s osobou, kterou dobře znám. Proto jsou mnohdy opomíjena rizika, která zdánlivě bezpečná výměna intimních materiálů přináší. Například po ukončení vztahu může dojít k vydírání dříve blízké osoby, že vše zveřejní.

Materiály zveřejněné v prostředí internetu prakticky nelze zcela beze stopy odstranit. Mohou se opakovaně náhodně objevovat na internetu neomezeně dlouho, to může mít negativní dopady např. při navazování nového vztahu nebo při ucházení se o zaměstnání. Každý by měl proto opravdu zvážit komu a jaké intimní informace zasílá. Rozhodně by na fotografiích nemělo být vidět do obličeje a neměla by být patrná unikátní tetování či mateřská znaménka, podle čeho je možné člověka identifikovat.

Poškozená osoba by pod nátlakem a vyhrožováním neměla zasílat útočníkovi žádné další materiály. Málo lidí ví o možnosti požadovat po administrátorovi webu smazání daných materiálů. V závažných případech je však nezbytné celou věc řešit s policí. V takovém případě je důležité uchovat veškerou komunikaci zaslanou mezi útočníkem a obětí.

por. Bc. Monika Schindlová, DiS.

64. Podvody na internetových inzertních portálech

Online ● pribramsko.eu (Regionální zprávy) ● 4. 10. 2022, 9:41

Dosah: 739 ● GRP: 0.01 ● OTS: 0.00 ● AVE: 4577.33 Kč

Odkaz: https://pribramsko.eu/podvody-na-internetovych-inzertnich-portalech-12270

www.turistika-brdy.cz | www.ohkpb.cz | www.kdno.cz |

Příbramsko.eu

Server www.pribramsko.eu byl založen 13. května 2008

Dobré dopoledne, je úterý 4.10.2022, 9:46. Dnes má sv

Zprávy | Hydepark | Kultura a sport | Zdravý životní styl | Historie | Kontakty

Podvody na internetových inzertních portálech

2022-10-04 09:11:15 | PČR, por. Bc. Monika Schindlová, DiS. ©

Říjen je měsícem kybernetické bezpečnosti. Určitě je vhodné připomenout, jaká úskalí s sebou digitální prostředí přináší. Minulý týden přijali policisté na Příbramsku během čtyř dnů oznámení o pěti případech reverzních inzertních podvodů.

(Ilustrační foto archiv)

Většinou se jedná o podobný scénář. Pachatel zareaguje na váš inzerát. V oznámených případech šlo o prodej kopaček, oblečení, autobaterie, sedací soupravy a historických hrníčků. Falešný kupující předstírá zájem o prodávané zboží. Následně vám nabídne zajištění veškerého komfortu spojeného s přepravou i platbou a zašle vám fiktivní odkaz zpravidla na přepravní společnost.

Pokud na něj prodávající klikne, je přesměrován na podvrženou platební bránu, kde pak vyplní citlivé bankovní údaje, údaje k platební kartě. Místo připsaných peněz z prodeje zboží ale poté zjistí, že mu naopak na účtu chybí část jeho úspor. V uvedených pěti případech se jednalo o částku téměř dvě stě tisíc korun.

Terčem útočníků jsou zejména prodávající, kteří si zvolili platební metodu – zasílání peněz z karty na kartu prostřednictvím peněženky zvoleného bazaru. Prodávající nepředpokládají, že se z nich snaží někdo získat přístupové údaje k účtům a do internetového bankovnictví. Mají zájem zboží prodat co nejdříve, a proto slepě spolupracují.

Jak se podvodníkům bránit?

Důležité je vědět, že neklikám na odkazy do internetového bankovnictví obdržené v SMS zprávě či e-mailu. V žádném případě ani nepřeposílám autorizační kódy a za žádných okolností neposkytuji vzdálený přístup k počítači. Občané si také nyní mohou vyzkoušet interaktivní www.kybertest.cz, který je zábavnou formou seznámí s nejčastějšími kybernetickými podvody a naučí je, jak je rozpoznat a jak jim nenaletět.

To nevymažeš!

Dalším nebezpečím v digitálním prostředí je **sexting**. Jde o sdílení vlastních intimních fotografií či videí velmi často s osobou, kterou dobře znám. Proto jsou mnohdy opomíjena rizika, která zdánlivě bezpečná výměna intimních materiálů přináší. Například po ukončení vztahu může dojít k vydírání dříve blízké osoby, že vše zveřejní.

Materiály zveřejněné v prostředí internetu prakticky nelze zcela beze stopy odstranit. Mohou se opakovaně náhodně objevovat na internetu neomezeně dlouho, to může mít negativní dopady např. při navazování nového vztahu nebo při ucházení se o zaměstnání. Každý by měl proto opravdu zvážit komu a jaké intimní informace zasílá. Rozhodně by na fotografiích nemělo být vidět do obličeje a neměla by být patrná unikátní tetování či mateřská znaménka, podle čeho je možné člověka identifikovat.

Poškozená osoba by pod nátlakem a vyhrožováním neměla zasílat útočníkovi žádné další materiály. Málo lidí ví o možnosti požadovat po administrátorovi webu smazání daných materiálů. V závažných případech je však nezbytné celou věc řešit s policí. V takovém případě je důležité uchovat veškerou komunikaci zaslanou mezi útočníkem a obětí.

65. Žena ze Strakonic přišla o desítky tisíc. Odhalili byste kybernetický podvod vy? Zkuste test

Online ● jcted.cz (Regionální zprávy) ● 4. 10. 2022, 11:17

Vydavatel: **Jihočeské týdeníky s.r.o. (cz-26097346)** ● Autor: **Monika Prokýšková**

Dosah: 7 692 ● GRP: 0.09 ● OTS: 0.00 ● AVE: 13778.71 Kč ● Interakcí: 8

Odkaz: https://www.jcted.cz/68566-zena-ze-strakonic-prisla-o-desitky-tisic-odhalili-byste-kyberneticky-podvod-vy-zkuste-test/

Žena ze Strakonic přišla o desítky tisíc. Odhalili byste kybernetický podvod vy? Zkuste test

4.10.2022 11:17

STRAKONICE - O 35 tisíc korun přišla pětačtyřicetiletá žena ze Strakonic, kterou oslovil na portálu Vinted podvodník předstírající zájem o zboží, které zde nabízela. Vylákal z ní potřebné přístupové údaje k platební kartě a vybral její konto. Zda byste dokázali rozpoznat podvod si můžete vyzkoušet v testu, vzkazuje policie.

Podvodník, tvářící se jako zájemce o koupi zboží, které žena nabízela, tvrdil, že k tomu, aby údajně mohl dokončit objednávku, potřebuje její e-mailovou adresu. Na tu jí následně zaslal zprávu obsahující podvodný odkaz. „Žena v odkazu odsouhlasila kolonku potvrdit prodej, což jí přesměrovalo na podvodné stránky portálu Vinted, kde pro dokončení měla vyplnit údaje ke své platební kartě. Tímto způsobem od ženy pachatel vylákal potřebné přístupové údaje k platební kartě a už mu nic nechybělo, aby provedl neoprávněné transakce," popsala mluvčí strakonické policie Jaromíra Nováková.

Přestože policisté o podobných případech veřejnost neustále informují a varují, stále jsou pachatelé úspěšní. „Nikdy nikomu nesdělujte a nevypisujte svá hesla a přístupové údaje. Útoků na vaše peníze přibývá a jsou pořád rafinovanější. Zda byste dokázali podvodné praktiky kybernetického útočníka rozpoznat a nenaletět, si můžete vyzkoušet ve vzdělávacím testu www.kybertest.cz," varuje znovu Jaromíra Nováková.

66. Policie radí, jak se bránit podvodům na internetu či sextingu

Online ● zpravypribram.cz (Regionální zprávy) ● 4. 10. 2022, 11:50

Rubrika: **Krimi**

Dosah: 255 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 2466.00 Kč

Odkaz: https://www.zpravypribram.cz/policie-radi-jak-se-branit-podvodum-na-internetu-ci-sextingu/

PŘÍBRAMSKO – Říjen je měsícem kybernetické bezpečnosti. Určitě je vhodné připomenout, jaká úskalí s sebou digitální prostředí přináší. Minulý týden přijali policisté na Příbramsku během čtyř dnů oznámení o pěti případech reverzních inzertních podvodů.

Většinou se jedná o podobný scénář. Pachatel zareaguje na váš inzerát. V oznámených případech šlo o prodej kopaček, oblečení, autobaterie, sedací soupravy a historických hrníčků. Falešný kupující předstírá zájem o prodávané zboží. Následně vám nabídne zajištění veškerého komfortu spojeného s přepravou i platbou a zašle vám fiktivní odkaz zpravidla na přepravní společnost. Pokud na něj prodávající klikne, je přesměrován na podvrženou platební bránu, kde pak vyplní citlivé bankovní údaje, údaje k platební kartě. Místo připsaných peněz z prodeje zboží ale poté zjistí, že mu naopak na účtu chybí část jeho úspor. V uvedených pěti případech se jednalo o částku téměř dvě stě tisíc korun.

Terčem útočníků jsou zejména prodávající, kteří si zvolili platební metodu – zasílání peněz z karty na kartu prostřednictvím peněženky zvoleného bazaru. Prodávající nepředpokládají, že se z nich snaží někdo získat přístupové údaje k účtům a do internetového bankovnictví. Mají zájem zboží prodat co nejdříve, a proto slepě spolupracují.

Jak se podvodníkům bránit? Důležité je vědět, že neklikám na odkazy do internetového bankovnictví obdržené v SMS zprávě či e-mailu. V žádném případě ani nepřeposílám autorizační kódy a za žádných okolností neposkytuji vzdálený přístup k počítači. Občané si také nyní mohou vyzkoušet interaktivní www.kybertest.cz, který je zábavnou formou seznámí s nejčastějšími kybernetickými podvody a naučí je, jak je rozpoznat a jak jim nenaletět.

Dalším nebezpečím v digitálním prostředí je sexting. Jde o sdílení vlastních intimních fotografií či videí velmi často s osobou, kterou dobře znám. Proto jsou mnohdy opomíjena rizika, která zdánlivě bezpečná výměna intimních materiálů přináší. Například po ukončení vztahu může dojít k vydírání dříve blízké osoby, že vše zveřejní.

Materiály zveřejněné v prostředí internetu prakticky nelze zcela beze stopy odstranit. Mohou se opakovaně náhodně objevovat na internetu neomezeně dlouho, to může mít negativní dopady např. při navazování nového vztahu nebo při ucházení se o zaměstnání. Každý by měl proto opravdu zvážit komu a jaké intimní informace zasílá. Rozhodně by na fotografiích nemělo být vidět do obličeje a neměla by být patrná unikátní tetování či mateřská znaménka, podle čeho je možné člověka identifikovat.

Poškozená osoba by pod nátlakem a vyhrožováním neměla zasílat útočníkovi žádné další materiály. Málo lidí ví o možnosti požadovat po administrátorovi webu smazání daných materiálů. V závažných případech je však nezbytné celou věc řešit s policí. V takovém případě je důležité uchovat veškerou komunikaci zaslanou mezi útočníkem a obětí.

por. Bc. Monika Schindlová, DiS,

komisař prevence

67. Železničář, číslo 10/2022; str. 27

Tisk ● Železničář; str. 27 (Jiné) ● 6. 10. 2022

Vydavatel: **České dráhy, a.s. (cz-70994226)**

Dosah: 10 500 ● GRP: 0.12 ● OTS: 0.00

Odkaz: náhled

68. Pachatel opět vylákal údaje k platební kartě. Žena ze Strakonic přišla o 35 tisíc korun

Tisk • Strakonický deník; str. 2 (Regionální zprávy) • 6. 10. 2022

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)**

Dosah: 3 356 • GRP: 0.04 • OTS: 0.00 • AVE: 6236.08 Kč

Odkaz: náhled

STRAKONICKO | Jižní Čechy

ČTENÁŘ REPORTÉR deník

Tip na výlet Miroslava Fialy

Putování Svatojakubskou cestou až na Blaník

Tip na výlet nám tentokrát poslal Miroslav Fiala. Zavedl nás na Táborsko.

„Putoval jsem podél zlatonosné Blanice chráněným územím z Mladé Vožice přes oba Blaníky do Louňovic pod Blaníkem. Kráčel jsem po poutní svatojakubské trase zádumčivou krajinou pomalu se odívající do podzimního šatu, jež byla plná zajímavostí a historických památek.

Každým krokem jsem se nořil hlouběji do tajemné historie, až jsem skončil u Keltů na Blaníku. Asi by se divili, jak to tu dnes vypadá a těžko by poznávali známá místa.

Vydal jsem se tentokrát v rámci tradičního svatováclavského pochodu právě na Blaník, který je pověstí spojen se svatým Václavem a jeho vojskem ukrytým v hoře."

Hrad Šelmberk

Hrad založený pány ze Šelmberka před rokem 1318. V 15. století často měnil majitele a v polovině 16. století prodělal renesanční přestavbu. Křídlo nově postavené zámecké budovy přetnulo i hradní příkop. V 17. stol. se uvádí jako pustý.

Tvrz Kamberk

Tvrz, patřící k nejstarším tvrzím na území Podblanicka, byla založena asi ve 13. stol. Plnila zřejmě správní a obrannou funkci pro celou oblast těžby zlata. Byla původně v držení významného rodu pánů z Landštejna.

Malý Blaník

Jeho hřebenitý skalnatý vrchol tyčí se do výšky 580 m. Celý je pokryt mohutným bukovo-smrkovým porostem s kamenitým podložím složeným převážně z tzv. blanické ortoruly. Je to i významné poutní místo tvořené kaplí sv. Máří Magdaleny z roku 1753, z níž se dochovaly jen trosky.

Velký Blaník

Bájný vrch s nadmořskou výškou 638 m. V lesích nalezneme mohutné kamenné valy, pozůstatky keltského oppida se dvěma řadami kamenných valů, později tvrz. Na vrcholu stojí dřevěná rozhledna vysoká 32 m. Blaník je již neodmyslitelně spojen s pověstmi o sv. Václavu a jeho rytířích ukrytých v nitru hory.

Více fotek naleznete na **www.strakonicky.denik.cz** v rubrice **Čtenář reportér**.

www.strakonicky.denik.cz

Jihočeští policisté zvládají víceboj i záchranu tonoucího

V plné polní v těžkém terénu? „Říkal jsem si, že jsem ze Šumavy a jsem zvyklý, ale bylo to horší než běžet na Libín," popisuje prachatický policista Josef Předota.

JANA VANDLÍČKOVÁ

Být policistou neznamená jen „Pomáhat a chránit". Policisté z přímého výkonu měří také pravidelně své síly s kolegy z celé republiky. Jedna taková soutěž se ve druhém zářijovém týdnu odehrála v Ostrově u Tisé. Šlo o policejní mistrovství ve víceboji a záchraně tonoucího. „Závody vycházejí ze služby, kterou policisté vykonávají přímo na ulici. Nejde tedy jen o pronásledování zločinců, ale také o záchranu života tonoucího, což byla protentokrát jedna z disciplín," vysvětluje Josef Předota, který byl pověřeným šéfem reprezentačního týmu Krajského ředitelství policie v Českých Budějovicích. Tým jihočeských policistů skončil letos na celkovém pátém místě. V celkovém hodnocení bral v kategorii nad 45 let David Hrádek z Jindřichova Hradce druhé místo a Josef Předota z Prachatic místo čtvrté.

V hodnocení jednotlivců získal Josef Předota ve své kategorii 1. místo ve střelbě a 3. místo v záchraně tonoucího. David Hrádek byl první v terénním běhu a na překážkové dráze. Stejně jako Patrik Kilián z Českých Budějovic byl první v terénním běhu v kategorii nad 35 let a 4. místo obsadil ve střelbě v kategorii nad 35 let Jan Šíma z Prachatic.

Součástí jihočeského týmu byli čtyři policisté všech věkových kategorií. „Já osobně jsem už veterán," směje se a dodává, že závod je složený z pěti disciplín. Jde o taktickou střelbu, se kterou se může policista setkat při přestřelce s pachatelem. Další disciplínou je překážková dráha. „Ta je velmi náročná na fyzičku. Je dlouhá zhruba čtyři sta metrů a jde o čas. Její součástí jsou různé prolézačky, které se musejí přelézt, podlézt či jinak překonat. Náročný je rovněž běh terénem, plazení se, a to vždy v pracovním oděvu a kanadách. probíhá se i řekou," popisuje Josef Předota tu nejnáročnější disciplínu. O nic lehčí není ani záchrana tonoucího. V téhle disciplíně se policisté v oblečení, ovšem tentokrát bez obuvi, snaží zachránit život člověku ve vodě. Po trati, která je dlouhá 110 metrů, musí policisté k raftům. Ty jsou umístěné tak, že jeden je na hladině a druhý je otočený. Policista musí doběhnout a doplavat k jednomu a následně i ke druhému raftu a zachránit člověka. To se opakuje dvakrát. „V téhle disciplíně jsem byl třetí, ale musím říct, že mě to dost vyšťavilo. Fakt to bylo hodně náročné," popisuje. Čtvrtou disciplínou je pětikilometrový terénní běh v plné polní. Na téhle trati bylo obrovské převýšení. „Říkal jsem si, že jsem ze Šumavy a tudíž jsem zvyklý, ale bylo to snad horší než vyběhnout na Libín," přirovnává Josef Předota.

V poslední disciplíně musí tým společně uběhnout dvanáct kilometrů ve velmi náročném terénu. „Ve volném čase musím denně sportovat, jinak bych nebyl schopen to zvládnout. Navíc o tom, že pojedu, vím předem," vysvětluje Josef Předota, jak se připravuje. Republikových závodů se už zúčastnil minimálně desetkrát. Tým se pak sjede na soustředění ve středisku v Lišově. Jen tam mají jeho členové možnost se poznat osobně a zjistit, co jeden od druhého může čekat. Do té chvíle se mnohdy vůbec neznají. „Po soustředění je tým sladěný, což se následně odráží na výsledku," říká.

Josef Předota ujišťuje, že u policie má úplně každý možnost sportovat. Každoročně totiž policie pořádá závody v běžeckém lyžování, střelbě, florbalu nebo ve víceboji. Josef Předota je také částečně personalistou a nové kolegy láká právě na sport. „Ti, co mají sportování rádi, mají šanci se prosadit," uzavírá policista.

Policajt musí mít fyzičku. Josef Předota z Prachatic sportuje každý den. Říká, že jinak není schopný policejní závody zvládnout. Týden soustředění je málo.

JSOU TÝM. Jihočeši před samotným závodem absolvovali soustředění v Lišově. Nahoře zleva Patrik Kilián (ČB), Jan Šíma (PT), Petr Šlejhar (ČB), trenér Pavel Strnad (ČB). Dole zleva šéf týmu Josef Předota (PT), Jana Hanžlová (PT), Iveta Duchoňová (PT) a David Hrádek (JH). Foto: Policie ČR

ZLATO. Josef Předota si přivezl medaili za nejlepší střelbu.

Pachatel opět vylákal údaje k platební kartě. Žena ze Strakonic přišla o 35 tisíc korun

PETR ŠKOTKO

Strakonice – O třicet pět tisíc korun přišla žena (45) ze Strakonic.

Ženu oslovil neznámý pachatel na portálu Vinted, kde předstíral zájem o zboží, které zde nabízela. Aby údajně mohl dokončit objednávku, požadoval po ženě zaslání e-mailové adresy, na kterou jí následně zaslal zprávu obsahující podvodný odkaz. Žena v odkazu odsouhlasila „potvrdit prodej", což ji přesměrovalo na podvodné stránky portálu Vinted, kde pro dokončení měla vyplnit údaje ke své platební kartě. „Tímto způsobem od ženy pachatel vylákal potřebné přístupové údaje k platební kartě a už mu nic nechybělo, aby provedl neoprávněné transakce," řekla tisková mluvčí strakonické policie Jaromíra Nováková.

Přestože policisté o případech občany neustále informují a varují, stále jsou pachatelé úspěšní. Nikdy nikomu nesdělujte a nevypisujte svá hesla a přístupové údaje. „Útoků na vaše peníze přibývá a jsou stále rafinovanější," dodala mluvčí.

Zda byste dokázali podvodné praktiky kybernetického útočníka rozpoznat a nenaletět, si můžete vyzkoušet ve vzdělávacím testu www.kybertest.cz. Vyzkoušejte si tento test nejen vy sami, ale doporučte ho také svým kamarádům a známým. Pomůžete tak snížit riziko okradení. **(pš)**

Zkušenost

Muž ze Strakonicka prodával na internetu ještě zachovalé matrace. „Čekal jsem, že někdo zavolá, zeptá na cenu a pak se domluvíme. Místo toho po mně dva zájemci chtěli číslo karty, navýšení možností výběru a pak potvrzení objednávky. Vypadalo to docela přesvědčivě, naštěstí je ve zprávách i v novinách popsána celá řada podvodů." Díky tomu, že „úkol nesplnil", měli údajní zájemci smůlu a na účet se nedostali.

DENÍK V JIHOČESKÝCH MUTACÍCH: Českobudějovický deník, Českokrumlovský deník, Prachatický deník, Strakonický deník, Písecký deník, Táborský deník, Jindřichohradecký deník. Vychází pondělí – sobota. Vydává VLTAVA LABE MEDIA a.s., U Trezorky 921/2, Jinonice, 158 00 Praha 5, IČ 01440578. Předseda představenstva a generální ředitel: Vít Nantl. CENTRÁLNÍ REDAKCE: U Trezorky 921/2, Jinonice, 158 00 Praha 5. Od 1. 1. 2022 je platný ceník inzerce č. 22.
REGION JIŽNÍ ČECHY: Náměstí Přemysla Otakara II. 8/5, 370 01 České Budějovice. **Manažer inzerce:** Pavla Pudivítrová, e-mail: pavla.pudivitrova@vlmedia.cz. Šéfredaktor redakcí v jižních Čechách: Kamil Kacerovský, šéfeditor redakcí v jižních Čechách: Martin Tröster.
STRAKONICKÝ DENÍK: Náměstí Přemysla Otakara II. 8/5, 370 01 České Budějovice, redakce.strakonicky@denik.cz. **Šéfredaktor Strakonického deníku:** Petr Škotko, e-mail: petr.skotko@denik.cz, mobil: 724 020 786. **Příspěvky čtenářů:** Klára Alešová, mobil: 602 667 620, e-mail: klara.alesova@denik.cz. **Sport:** Vladimír Klíma, e-mail: vladimir.klima@denik.cz, mobil: 602 667 613. **Manažer distribuce:** Roman Dvořák, e-mail: roman.dvorak@denik.cz. **Inzerce:** Miroslava Žížková, e-mail: miroslava.zizkova@denik.cz, tel.: 724 020 784. **Servis pro čtenáře, řádková inzerce:** inzerce.radkova.JC@vlmedia.cz. Texty označené PR, PI jsou placená inzerce. **Tiskne:** VLTAVA LABE MEDIA a.s., tiskárna Novotisk Praha. Ročník XVIII, ISSN 1210-7352, MK ČR E6566. Prodaný náklad ověřuje ABC ČR, Pobřežní 370/4, 186 00 Praha 8. Nevyžádané rukopisy a fotografie se nevracejí. Předplatné doručuje Mediaservis, s.r.o. Deník najdete také v aplikacích pro iPhone a OS Android. **Centrum zákaznické péče: 272 015 015, 272 015 020.** E-mail: denik@mojepredplatne.cz, více: www.mojepredplatne.cz. V případě reklamace doručení nás, prosím, kontaktujte na el. adrese: reklamace@denik.cz.

69. Pachatel opět vylákal údaje ke kartě. Žena ze Strakonic přišla o 35 tisíc

Online ● strakonicky.denik.cz (Regionální zprávy) ● 6. 10. 2022, 8:18

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)** ● Autor: **Petr Škotko** ● Rubrika: **Zprávy**

Dosah: 2 596 ● GRP: 0.03 ● OTS: 0.00 ● AVE: 8632.04 Kč ● Interakcí: 3

Odkaz: https://strakonicky.denik.cz/zpravy_region/pachatel-opet-vylakal-udaje-ke-karte-zena-ze-strakonic-prisla-o-35-tisic-2022100.html

70. Kybertest poběží až do konce roku. Zapojit se může každý

Tisk ● Bankovnictví; str. 54, 55 (Ekonomika / Finance / Právo) ● 7. 10. 2022

Vydavatel: **4H production s.r.o. (cz-28471831)** ● Rubrika: **BANKY A FINANCE**

Dosah: 12 248 ● GRP: 0.14 ● OTS: 0.00 ● AVE: 158000.00 Kč

Odkaz: náhled

BANKY A FINANCE
KYBERNETICKÁ BEZPEČNOST

Kybertest poběží až do konce roku. Zapojit se může každý

Začátkem září představila Česká bankovní asociace celonárodní vzdělávací kampaň v oblasti kyberbezpečnosti – #nePINdej! Spolu s ní také představila další z řady testů znalostí v oblasti kyberbezpečnosti, který je klíčovým prvkem celé kampaně a se kterým bude v následujících měsících intenzivně pracovat.

Podle dat České bankovní asociace se počet útoků na klienty bank za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů a na jednoho poškozeného klienta je to v průměru 161 500 korun. „Jen za prvních sedm měsíců letošního roku byl počet útoků na klienty bank dvojnásobně vyšší než za celý loňský rok. Dramaticky přitom narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším. Zatímco před dvěma lety se jejich počet pohyboval v nízkých stovkách, letos mluvíme již o desítkách tisíc. A narostla i jejich úspěšnost. Téměř každý druhý podvodný telefonát v současné době bohužel končí škodou pro klienta. Průměrné částka, o kterou klienti při těchto útocích přijdou, je přitom dost vysoká, zhruba čtvrt milionu korun," uvedla Monika Zahálková, výkonná ředitelka České bankovní asociace. Její slova potvrzuje i Lukáš Kintr, ředitel Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). „Žijeme v digitální době, která nám mnohé věci usnadňuje, ale také přináší mnohá rizika a mezi ně patří i rostoucí počet různých kyberútoků. Detekujeme vysoké počty nejen podvodných telefonátů, ale i textových zpráv či e-mailů, a nelze očekávat, že by se jejich míra měla snižovat. Nejlepší obranou proti těmto pokusům nadále zůstává obecná osvěta, tedy informovanost a poučenost veřejnosti, aby byli lidé schopni vishing a podobné snahy rozpoznat," upřesňuje Lukáš Kintr.

#nePINdej! aneb společně proti kyberkriminalitě

Právě díky výše zmíněným faktům představila ČBA spolu s partnery nejen z finanční sféry výše zmíněnou kampaň #nePINdej!. Právě ta skrze hravý kybertest představí nejčastější kybernetické útoky a zároveň klienty naučí, jak těmto podvodům nenaletět.

Samotný kybertest má za cíl oslovit širokou veřejnost od mladistvých až po seniory. Také proto má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin a pohlaví. „Jiné otázky se tedy generují pro teenagery, jiné pro seniory. Stejně tak jako útoky hackerů – jiné praktiky zkoušejí na mladší generaci, jiné pak na střední a jiné na nejstarší spoluobčany," vysvětluje Tomáš Trachta, člen představenstva společnosti itego, a.s., která pro ČBA kybertest naprogramovala a úzce spolupracovala na realizaci celé kampaně. Po spuštění testu dostane každý jeho účastník virtuální peníze do „hry", které musí před podvodnými útoky co nejlépe ochránit. Po každé otázce se lidé dozvědí správné řešení, mohou se z něj tak poučit a dalšímu simulovanému útoku následně nenaletět.

Samotný kybertest má za cíl oslovit širokou veřejnost od mladistvých až po seniory. Také proto má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin a pohlaví.

Od spuštění testu ČBA sleduje statistiky, kolik lidí si test již udělalo. „Z nich vyplývá, že denně si ho dělá více než tisíc lidí, což považujeme za skvělý úspěch. Zájem neopadá, ba právě naopak," uvádí Monika Zahálková.

Kybertest doplní Bankéře do škol

Současná podoba testu není konečná. Jak upřesnila Monika Zahálková, ČBA na samotné aplikaci neustále pracuje. „Rozvíjíme ji, zlepšujeme. A v tom budeme pokračovat i nadále. Pokud se týká komunikace, nyní nám běží kampaň například ve vybraných kinech CineStar, na nádražích Českých drah, na pobočkách České pošty rozdáváme letáky pro „off-line" seniory a začali jsme i kampaň na sociálních sítích a u našich mediálních partnerů. Hlavním mediálním partnerem je Česká televize, tam poběží spoty v listopadu. S kybertestem jdeme v říjnu i do škol v rámci našeho projektu Bankéři do škol. Podporu nám ve školách slíbilo i O2, stejně tak i formou SMS zpráv," upřesnila Monika Zahálková s tím, že kampaň poběží až do konce roku. „To v praxi znamená, že ještě řadu aktivit připravujeme a budeme je postupně nasazovat. Například i CLV televize v MHD ve vybraných krajských městech atd."

Co se týče zapojení samotných bank, ty se pak mají možnost angažovat zejména v oblasti komunikace. „Finanční instituce se v kampani angažují prostřednictvím ČBA, která je organizátorem celého projektu, a tudíž má klíčovou roli. Jednotlivé banky se do projektu zapojují i jinak – komunikují ho například na svých pobočkách, bankomatech a sociálních sítích," upřesnila Monika Zahálková.

Co se dalších finančních institucí týče (pojišťovny, nebanky atd.), ty mají prozatím smůlu, i když ČBA s nimi do budoucna spolupráci nevylučuje.

Největší kyberbezpečnostní kampaň v Česku

Kampaň #nePINdej! zcela jistě patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud v České republice realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají. Kromě České bankovní asociace, která je realizátorem projektu, jsou do kampaně zapojeny Policie České republiky, Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), itego, a.s., CISCO, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy.

B | Text Redakce
www.bankovnictvionline.cz

Ani dvoufaktorové ověření klienta nemusí ochránit

Jak už bylo řečeno, mezi nejčastější útoky dnes patří phishing (útočník se vydává za důvěryhodnou autoritu s cílem získat citlivá data oběti), smishing (forma phishingu – jedná se také o podvodnou praktiku, která má za cíl vylákat z cílové osoby citlivé údaje, ale na rozdíl od phishingu využívá nejčastěji SMS) a vishing (tzv. hlasový phishing nebo voice phishing – jedná se o podvod, při kterém se útočníci snaží vylákat z oběti peníze prostřednictvím telefonního hovoru.) Ten je dle ČBA vůbec nejnebezpečnější, protože podvodníci umí napodobit telefonní číslo renomované instituce, dokážou dobře vystihnout moment překvapení a umí pracovat s lidským strachem – klienti, ve snaze ochránit své finance, vykonávají pokyny podvodníků a dávají jim přístupová hesla nebo vkládají své finance prostřednictvím vkladomatů na kryptoměnu na jejich účty.

Tyto typy útoků jsou od začátku postaveny na scénářích, kde je podmínkou získání spolupráce klienta (strach o peníze z důvodu napadení účtu, nabídka výhodného produktu v době inflace...). Není problém pro pachatele obejít i ověření přes druhý faktor. Stačí vytvořit jen správnou legendu, které klient uvěří, a pak buď sám přes svůj vlastní telefon nebo jiný autorizační prvek pachatelům peníze odešle, tedy vše sám potvrdí v domnění, že peníze převádí na „bezpečné místo v bance" (ve skutečnosti se ale jedná o účet pachatelů). Anebo si pachatelé s jeho pomocí nechají klientem pod připravenou legendou aktivovat vlastní autorizační prvek (svůj vlastní telefon) a s ním si pak platby potvrzují již sami. Stačí tedy například přesvědčit klienta, aby si sám nainstaloval do svého počítače aplikaci/program umožňující přístup do jeho počítače přes tzv. vzdálenou plochu pod legendou, že mu jako „pracovník banky" se vším rád a rychle pomohu, přes tento vzdálený přístup získat i přístup na účet klienta a pak už jen klientovi tvrdit, že je potřeba, aby na svém telefonu / ve své mobilní aplikaci potvrzoval vše, co mu bude z banky přicházet. Klient, protože se domnívá, že vše dělá pracovník banky, všemu důvěřuje, nic nečte a jen vše potvrzuje přes „zelené tlačítko". Výsledkem je pak to, že přijde o všechny své peníze, protože jejich odeslání autorizoval buď sám, anebo umožnil autorizaci tím, že sám povolil připojení jiného autorizačního zařízení ke svému účtu.

A právě zde je problém. Ačkoli banky investují nemálo peněz do rozvoje bezpečnostních systémů a jejich zabezpečení je na špičkové úrovni, selže zpravidla klient. To banky nemohou bezprostředně ovlivnit, ale snaží se o to osvětou a edukací, jako je třeba kybertest.

> Finanční instituce se v kampani angažují prostřednictvím ČBA, která je organizátorem celého projektu, a tudíž má klíčovou roli. Jednotlivé banky se do projektu zapojují i jinak – komunikují ho například na svých pobočkách, bankomatech a sociálních sítích.

71. Oběti kyberpodvodů se často diví, jak se nechaly obrat

Tisk ● Rakovnický deník; str. 2 (Regionální zprávy) ● 7. 10. 2022

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)**

Dosah: 47 353 ● GRP: 0.53 ● OTS: 0.01 ● AVE: 105439.49 Kč

Odkaz: náhled

ZPRAVODAJSTVÍ | Rakovnicko

Redaktor Deníku Jan Brabec doporučuje

Tipy deníku

Dům osvěty v Rakovníku rozduní hned čtveřice kapel

7. října | 19:00

Rakovník – Rakovnický Dům osvěty bude v pátek 7. října hostit další z koncertů. Tentokrát v jeho prostorách vystoupí hned čtveřice kapel. Příchozí se mohou těšit na hudbu v podání skupin Smečka (rock-metal, Nové Křečany), Sethorus (melodic-rock, Praha), Fret (hard rock-stoner rock, Rakovník) a Five Sins (rock-hard rock, Rakovník). Za vstupenky zájemci dají 120 korun.

ČTENÁŘ REPORTÉR deník

Nejčtenější: Studenti slavili Evropský den jazyků

Rakovník – *Nejčtenějším článkem Rakovnického deníku v rubrice Čtenář reportér za uplynulý týden byl ten o oslavě Evropského dne jazyků.* Žáci i učitelé Gymnázia Zikmunda Wintra oslavili Evropský den jazyků projektovým dnem plným hudby a zpěvu. V dopoledních hodinách jsme se postupně po jazykových skupinách scházeli v tělocvičně a nacvičovali zpěv evropské hymny. Na hudební nástroje hráli žáci například z různých tříd. Notový materiál pro jednotlivé nástroje a celou hudební kompozici připravila Aneta Matoušková, žákyně kvinty. Pod vedením mgr. Elznicové a mgr. Prachařové, učitelek hudební výchovy, nás všechny dojímal tento báječný orchestr tóny závěrečné věty Deváté symfonie Ludwiga van Beethovena. Všichni žáci se naučili textové verze hymny v těch jazycích, které na gymnáziu vyučujeme. Po sladění zpěvu a hudby jsme vyšli před kostel sv. Bartoloměje, abychom na chvíli oživili veřejný prostor a uspořádali jsme flashmob. *Celý článek a více snímků naleznete na webu* ***www.rakovnicky.denik.cz***. Autor: O. Beulakerová, GZW Rakovník

KRÁTCE Z REGIONU

Narodili se

Rakovnicko – Ve spolupráci s porodnicí Masarykovy nemocnice v Rakovníku vám přinášíme přehled dětí z Rakovnicka narozených v minulých dnech.

30. září – Matyáš František **Pouzar** (Rakovník), 30. září – Karolína **Palivcová** (Kroučová), 2. října – Jonáš **Dvořák** (Rakovník), 2. října – Adam **Ducár** (Třtice), 2. října – Tobiáš **Červený** (Nové Strašeci), 4. října – Nikita **Rejpaši** (Lužná), 4. října – Adam **Petrovický** (Rakovník), 5. října – Milana **Tseha** (Nesuchyně)

Opustili nás

Rakovnicko – Ve spolupráci s pohřební službou Memoria Rakovník přinášíme jména zemřelých.

Josef **Havlica** (1937, Hředle), Jaroslav **Chaloupková** (1943, Rakovník), Petr **Krob** (1948, Nesuchyně), Hana **Hudíková** (1936, Kroučová), Alois **Jiruš** (1937, Hředle)

Oběti kyberpodvodů se často diví, jak se nechaly obrat

MILAN HOLAKOVSKÝ

Podvodů na internetu valem přibývá. Jen na Příbramsku přijali policisté během jediného týdne, vlastně za čtyři dny, oznámení o pěti takových případech. A jinde v kraji to není lepší. Nejčastější chyby, které lidé dělají, se přitom stále opakují: pachatelům sami poskytnou vše, co vykukové skrývající se ve spleti virtuálního světa potřebují.

Ilustrační foto. Deník

JEN OBYČEJNÉ NABÍDKY K PRODEJI

Zmiňovaná pětice případů, které nově řeší příbramská policie, se odehrála podle obdobného scénáře. Oběti se stali uživatelé inzertních serverů, kteří přišli o spoustu peněz, ačkoli měli původně v úmyslu pár korun získat prodejem různých věcí. Konkrétně šlo o nabídky kopaček, oblečení, autobaterie, sedací soupravy a historických hmátků.

Shodně ve všech případech kdosi na inzerát reagoval a vystupoval jako zájemce, ačkoli ve skutečnosti nic v úmyslu kupovat neměl. A pak už následoval osvědčený postup podvodníků: údajný kupec nabídne využití služby, jež prý nabízí veškerý komfort spojený s převodem i platbou. Zašle – zpravidla prostřednictvím aplikace WhatsApp – odkaz na web, který se zpravidla vydává za stránky skutečně existující přepravní společnosti. Nebo se tváří jako „peněženka" využitého internetového bazaru.

Tam je hlavní zádrhel. Prodávající je přesměrován na podvrženou platební bránu s pokynem, aby vyplnil údaje o své platební kartě. Byť sám nemá nic platit, ale naopak peníze dostat. Údajně je to proto, aby mu kupcem uhrazená částka mohla přijít přímo „na kartu". Ve skutečnosti podvodník získal přístup k penězům na účtu prodávajícího. O to mu šlo od počátku: chce ho připravit přinejmenším o část úspor. To se stalo i na Příbramsku: dohromady se jednalo o sumu dosahující téměř 200 tisíc korun. Není však výjimkou, že do statisíců šplhá v podobných případech výše škody i u jediného podvedeného.

Podvody toto typu se vzájemně podobají skoro jak přes kopírák. Terčem útočníků jsou zejména prodávající, kteří si jako platební metodu zvolili zaslání peněz na kartu. „Prodávající nepředpokládají, že se někdo snaží získat přístupové údaje. Mají zájem zboží prodat co nejdříve, a proto slepě spolupracují," vysvětlila Monika Schindlová z příbramského územního odboru středočeské policie. Stává se, že zpětně se lidé sami dívají tomu, jak si počínali.

K DISPOZICI JE TEST

Policie varuje, že v rámci ochrany proti podvodníkům je důležité vědět, že není radno klikat na odkazy do internetového bankovnictví obdržené třeba v SMS zprávě či e-mailem. A rozhodně nepřeposílat autorizační kódy k transakcím. Stejně jako v žádném případě neposkytovat vzdálený přístup k počítači. „Občané si také nyní mohou vyzkoušet interaktivní kybertest.cz, který je seznámí s nejčastějšími kybernetickými podvody a naučí je, jak je rozpoznat a jak jim nenaletět," upozornila Monika Schindlová.

Začíná velká oprava dálnice D1

JAN ŠINDELÁŘ

Osazováním omezujících značek zahájili minulý týden v pátek silničáři opravu šestiproruhového úseku dálnice D1 u Prahy mezi exity 15 (Všechromy) a 21 (Miroševice). Během opravy se bude na dálnici jezdit v provizorních pruzích v režimu 3+3. Výraznější bude provoz omezen ve dnech, kdy budou silničáři přesouvat omezující značení.

„V letošním roce proběhnou zejména připravné práce, hlavní stavební činnost je plánovaná na rok 2023," uvedl mluvčí Ředitelství silnic a dálnic (ŘSD) Martin Buček. Podzimní etapa prací potrvá podle aktuálních plánů do posledního listopadového víkendu. „V průběhu opravy realizované na podzim dojde pouze k lokálním posunům jízdních pruhů v místech prací směrem ke krajnici nebo naopak ke střednímu dělicímu pásu, aby byl vymezen bezpečný prostor pro pracovníky," doplnil Buček.

ÚSEK DÁLNICE mezi Mirošovicemi a Všechromy. Foto: zdopravy/ŘSD

Stavbaři budou pracovat například na provizorním přejezdu středního dělicího pásu, protihlukových stěnách u odpočívky Božkov nebo na mostě (ev. č. D1-018).

Kvůli pracím pod tímto mostem ŘSD původně plánovalo úplnou uzavírku silnice III/1016 mezi Kunicemi a Strančicemi. Rozhodnutí ale změnilo a nakonec zvolilo kyvadlovou dopravu řízenou semaforem, a to do konce listopadu.

Práce budou pokračovat na jaře, celková doba oprav má být 300 dnů. Zakázku získala společnost Eurovia s cenou 388 milionů korun, když předpoklad ŘSD byl 402 milionů.

Železniční den láká nejen milovníky vlaků

Střední Čechy – Železniční den se v Příbrami uskuteční v sobotu. Navzdory názvu si na své přijdou nejen milovníci vlaků, ale i autobusů. Železniční nádraží se ale stane centrem všeho dění.

Mezi 10. a 18. hodinou si zájemci budou moci užívat jízd historickými vlaky i autobusy, ale také doprovodného programu. Včetně výletů na zajímavá místa v Příbrami i okolí. Poloviční slevu ze vstupného nabídnou hornické muzeum a jeho Památník Vojna, areál dolu Rimbaba včetně vyhlídkové věže, vyhlídková věž Rudolfka, bohutínský mlýn, ale i muzeum na Svaté Hoře nebo Památník Antonína Dvořáka.

Z Prahy do Březnice vyjede na svou trasu výletní vlak Cyklo Brdy s patrovými vozy taženými lokomotivou Bardotka – tentokrát vlak před podvečerním návratem do hlavního města bude ještě mířit do Březnic, Příbrami a Jinců.

HISTORICKÉ AUTOBUSY

Další historický vlak, motorový vůz v retro nátěru, bude vozit cestující na vlečce do příbramských Kovohuti. Od nádraží budou také vyjíždět tři historické autobusy, které na čtyřech linkách dovezou zájemce na místa lákající k návštěvě. Svezení těmito autobusy bude zdarma – a právě v nich lze získat poukázky na slevu ze vstupného.

Vlakové nádraží v Příbrami chystá i další nabídku: od skákacího hradu pro děti přes stánky s občerstvením nebo s předměty s dopravní tématikou až po představení chystané integrace městské hromadné dopravy v Příbrami do systému PID. Děti i dospělé zde také jistě nadchne možnost vyzkoušet si jízdu na pákové drezíně nebo omrknout výstavu kolejových vozidel. Příležitost dozvědět se spoustu zajímavostí zase nabídnou komentované prohlídky pracoviště výpravčího nebo expozice o historii trati Zdice–Protivín. V rámci jízd zvláštních vlaků do Březnice bude možné navštívit také železniční muzeum U Koleji v Tochovicích.

TRAŤ ZDICE–PROTIVÍN

„Železniční den v Příbrami se koná zejména v souvislosti se zajímavou historií výstavby trati Zdice–Proti-vín," připomněl vedoucí příbramského kulturního centra Vlastimil Ševr. S tím, že zbudováním byla v květnu 1874 pověřena firma železničního podnikatele a březnického rodáka inženýra Jana Muziky. „Projekčně připravená trať byla vystavěna a otevřena již v prosinci následujícího roku, což dokládá úžasnou šikovnost a neuvěřitelně pracovní nasazení březnické firmy," konstatoval. **(hol)**

DENÍK VE STŘEDOČESKÝCH MUTACÍCH: Benešovský deník, Berounský deník, Kolínský deník, Kutnohorský deník, Mělnický deník, Mladoboleslavský deník, Nymburský deník, Příbramský deník, Rakovnický deník. Vychází pondělí – sobota. Vydává VLTAVA LABE MEDIA a.s., U Trezorky 921/2, Jinonice, 158 00 Praha 5, IČ 01440578. Předseda představenstva a generální ředitel: Vít Nantl. CENTRÁLNÍ REDAKCE: U Trezorky 921/2, Jinonice, 158 00 Praha 5. Od 1. 1. 2022 je platný ceník inzerce č. 22.
REGION STŘEDNÍ ČECHY: U Trezorky 921/2, Jinonice, 158 00 Praha 5. **Manažer inzerce:** Vít Hosálek, e-mail: vit.hosalek@vltavalabe.cz, mobil: 602 376 868. Šéfredaktor redakcí ve středních Čechách: Martin Rumler, šéfeditor redakcí ve středních Čechách: Martin Vaněk.
RAKOVNICKÝ DENÍK: U Trezorky 921/2, Jinonice, 158 00 Praha 5, e-mail: redakce.rakovnicky@denik.cz. **Šéfredaktor Rakovnického deníku:** Josef Rod, e-mail: josef.rod@denik.cz, mobil: 724 538 788. **Příspěvky čtenářů:** Jan Brabec, mobil: 777 356 763, e-mail: jan.brabec@denik.cz.
Sport: Rudolf Muzika, e-mail: rudolf.muzika@denik.cz. **Manažer distribuce:** Walter Oberländer, e-mail: walter.oberlander@vltavalabe.cz. **Servis pro čtenáře, řádková inzerce:** inzerce.radkova.STC@vltavalabe.cz. Texty označené PR, PI jsou placená inzerce. **Tiskne:** VLTAVA LABE MEDIA a.s., tiskárna Novotisk Praha. Ročník: XVIII, ISSN 1210-7352, MK ČR E6566. Prodaný náklad ověřuje ABC ČR. Pohřební 370/4, 186 00 Praha 8. Nevyžádané rukopisy a fotografie se nevracejí. Předplatné doručuje: Mediaservis, s.r.o. Deník najdete také v aplikacích pro iPhone a OS Android. **Centrum zákaznické péče: 272 015 015, 272 015 020.** E-mail: denik@mojepredplatne.cz, více: www.mojepredplatne.cz. V případě reklamace doručení nás, prosím, kontaktujte na el. adrese: reklamace@denik.cz.

72. Oběti podvodů na internetu se někdy samy diví, jak se nechaly obrat

Online ● pribramsky.denik.cz (Regionální zprávy) ● 7. 10. 2022, 7:14

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)** ● Autor: **Milan Holakovský**

Dosah: 1 523 ● GRP: 0.02 ● OTS: 0.00 ● AVE: 6682.50 Kč

Odkaz: https://pribramsky.denik.cz/zlociny-a-soudy/obeti-podvodu-na-internetu-se-nekdy-samy-divi-jak-se-nechaly-obrat-20221007.html

Oběti podvodů na internetu se někdy samy diví, jak se nechaly obrat

DNES 07:14

Milan Holakovský
Reportér
Napište mi

Podvodů na internetu valem přibývá. Jen na Příbramsku přijali policisté během jediného týdne, vlastně za čtyři dny, oznámení o pěti takových případech, připomněla Monika Schindlová z příbramského územního odboru středočeské policie.

Ilustrační foto. | *Foto: Pixabay*

Jinde v kraji to není lepší. Nejčastější chyby, které lidé dělají, se přitom stále opakují: pachatelům sami poskytnou vše, co vykukové skrývající se ve spleti virtuálního světa potřebují.

Jen obyčejné nabídky k prodeji

Zmiňovaná pětice případů, které nově řeší příbramská policie, se odehrála podle obdobného scénáře. Obětí se stali uživatelé inzertních serverů, kteří přišli o spoustu peněz, ačkoli měli původně v úmyslu pár korun získat prodejem různých věcí. Konkrétně šlo o nabídky kopaček, oblečení, autobaterie, sedací soupravy a historických hrníčků, upřesnila Schindlová.

Shodně ve všech případech kdosi na inzerát reagoval a vystupoval jako zájemce, ačkoli ve skutečnosti nic v úmyslu kupovat neměl. A pak už následoval osvědčený postup podvodníků: údajný kupec nabídne využití služby, jež prý nabízí veškerý komfort spojený s přepravou i platbou. Zašle – zpravidla prostřednictvím aplikace WhatsApp – odkaz na web, který se zpravidla vydává za stránky skutečně existující přepravní společnosti. Nebo se tváří jako „peněženka“ využitého internetového bazaru.

Noční jízda v protisměru po dálnici: řidička tak urazila skoro 32 kilometrů

PRECIST CLANEK ›

Tam je hlavní zádrhel. Prodávající je přesměrován na podvrženou platební bránu s pokynem, aby vyplnil údaje o své platební kartě. Byť sám nemá nic platit, ale naopak peníze dostat. Údajně je to proto, aby mu kupcem uhrazená částka mohla přijít přímo „na kartu". Ve skutečnosti připsáno nebude nic – podvodník ale získal přístup k penězům na účtu prodávajícího. O to mu šlo od počátku: chce ho připravit přinejmenším o část úspor. To se stalo i ve zmiňovaných pěti případech: dohromady se jednalo o sumu dosahující téměř dvou set tisíc korun. Není však výjimkou, že do statisíců šplhá v podobných případech výše škody i u jediného podvedeného.

Záludnosti prodávající neočekávají

Podvody toto typu se vzájemně podobají skoro jak přes kopírák. Terčem útočníků jsou zejména prodávající, kteří si jako platební metodu zvolili zaslání peněz na kartu, uvedla policistka Schindlová. „Prodávající nepředpokládají, že se někdo snaží získat přístupové údaje. Mají zájem zboží prodat co nejdříve, a proto slepě spolupracují," vysvětlila. Stává se, že zpětně se lidé sami diví tomu, jak si počínali.

Policie varuje, že v rámci ochrany proti podvodníkům je důležité vědět, že není radno klikat na odkazy do internetového bankovnictví obdržené třeba v SMS zprávě či e-mailem. A rozhodně nepřeposílat autorizační kódy k transakcím. Stejně jako v žádném případě neposkytovat vzdálený přístup k počítači. „Občané si také nyní mohou vyzkoušet interaktivní kybertest.cz, který je seznámí s nejčastějšími kybernetickými podvody a naučí je, jak je rozpoznat a jak jim nenaletět," upozornila Schindlová, že poučení, jak se na internetu nenapálit, lze získat právě prostřednictvím internetu: v tomto případě ale na stránkách spolehlivých a prověřených.

73. Další podvedený prodejce

Online ● policie.cz (Jiné) ● 9. 10. 2022, 11:23

Dosah: 20 667 ● GRP: 0.23 ● OTS: 0.00 ● AVE: 19996.45 Kč

Odkaz: https://www.policie.cz/clanek/dalsi-podvedeny-prodejce.aspx

ZPRAVODAJSTVÍ

Úvodní strana / Útvary Policie ČR / Krajská ře

Policie České republiky – KŘP Jihočeského kraje

Další podvedený prodejce

Tábor – Poškozená prodávala dětské kolo, přišla o téměř 200 000 korun. (Hlasová schránka 974 236 116)

Táborští policisté zahájili úkony trestního řízení ve věci přečinu podvodu. Poškozená prodávala přes známý internetový portál dětské jízdní kolo. Na WhatsApp jí přišla zpráva od osoby, vystupující pod jménem Olga, že by měla o kolo zájem. Ke zprávě pachatel také přiložil odkaz na službu Zásilkovny, přes kterou si prý bude moci utržené peníze vyzvednout a dále uvedl, že poté dorazí kurýr pro zboží. Poškozená přes zaslaný odkaz zadala svůj ID kód a přihlašovací údaje ke svému internetovému bankovnictví. Následně obdržela od banky zprávu o navýšení limitu pro výběr, o který sama nežádala. Do bankovnictví se již však nemohla přihlásit, její přihlašovací údaje nefungovaly, nemohla se ani dovolat do banky ze svého telefonního čísla, aby provedla zablokování karty. Toto se jí podařilo až z druhého telefonního čísla. Když se však k účtu konečně dostala, zjistila, že jí pachatel stačil převést peníze ze spořicího účtu na běžný a odtud peníze odcizit převedením na cizí účet, čímž jí způsobil škodu za téměř 200 000 korun. Dalších nejméně 120 000 korun si podvodník přichystal k převodu, to se mu však již díky blokaci účtu nepodařilo.

Základní rady, jak nenaletět

- Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.
- Vyzkoušej si **www.kybertest.cz** a zjisti, kde máš mezery. Buď připraven.

por. Bc. Martina Joklová, pt.pis@pcr.cz

9. října 2022

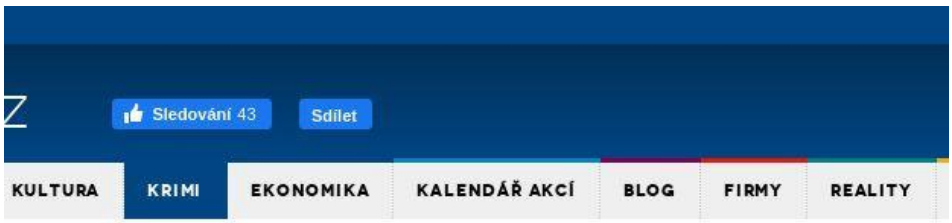
E-mailem Vytisknout

74. Další podvedený prodejce

Online ● regionjih.cz (Regionální zprávy) ● 9. 10. 2022, 11:23

Dosah: 34 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 860.70 Kč

Odkaz: https://www.regionjih.cz/zpravodajstvi/dalsi-podvedeny-prodejce-179541/



Další podvedený prodejce

Tábor – Poškozená prodávala dětské kolo, přišla o téměř 200 000 korun. (Hlasová schránka 974 236 116)

Táborští policisté zahájili úkony trestního řízení ve věci přečinu podvodu. Poškozená prodávala přes známý internetový portál dětské jízdní kolo. Na WhatsApp jí přišla zpráva

od osoby, vystupující pod jménem Olga, že by měla o kolo zájem. Ke zprávě pachatel také přiložil odkaz na službu Zásilkovny, přes kterou si prý bude moci utržené peníze vyzvednout a dále uvedl, že poté dorazí kurýr pro zboží. Poškozená přes zaslaný odkaz zadala svůj ID kód a přihlašovací údaje ke svému internetovému bankovnictví. Následně obdržela od banky zprávu o navýšení limitu pro výběr, o který sama nežádala. Do bankovnictví se již však nemohla přihlásit, její přihlašovací údaje nefungovaly, nemohla se ani dovolat do banky ze svého telefonního čísla, aby provedla zablokování karty. Toto se jí podařilo až z druhého telefonního čísla. Když se však k účtu konečně dostala, zjistila, že jí pachatel stačil převést peníze ze spořícího účtu na běžný a odtud peníze odcizit převedením na cizí účet, čímž jí způsobil škodu za téměř 200 000 korun. Dalších nejméně 120 000 korun si podvodník přichystal k převodu, to se mu však již díky blokaci účtu nepdoařilo. Základní rady, jak nenaletět Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech. Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli. Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý. Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze. Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou. Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu. Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ. Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty. Vyzkoušej si www.kybertest.cz a zjisti, kde máš mezery. Buď připraven. por. Bc. Martina Joklová, pt.pis@pcr.cz 9. října 2022

75. Prodávala dětské kolo. Místo toho přišla o 200 tisíc

Online ● taborsky.denik.cz (Regionální zprávy) ● 9. 10. 2022, 16:03

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)** ● Autor: **Jiří Dintar**

Dosah: 3 756 ● GRP: 0.04 ● OTS: 0.00 ● AVE: 10197.34 Kč ● Interakcí: 9

Odkaz: https://taborsky.denik.cz/zlociny-a-soudy/prodavala-detske-kolo-misto-toho-prisla-o-200-tisic-20221009.html

„Poškozená prodávala přes internetový portál dětské jízdní kolo. Na WhatsApp jí přišla zpráva od osoby, vystupující pod jménem Olga, že by měla o kolo zájem. Ke zprávě pachatel také přiložil odkaz na službu Zásilkovny, přes kterou si prý bude moci utržené peníze vyzvednout a dále uvedl, že poté dorazí kurýr pro zboží," popsala mluvčí jihočeských policistů Martina Joklová.

Žena poté přes zaslaný odkaz zadala svůj identifikační kód a přihlašovací údaje ke svému internetovému bankovnictví. Následně obdržela od banky zprávu o navýšení limitu pro výběr, o který sama nežádala.

Noční požár vyhnal z výrobní haly ve Velenicích přes šest desítek lidí

PŘEČÍST ČLÁNEK ›

„Do bankovnictví se již však nemohla přihlásit, její přihlašovací údaje nefungovaly, nemohla se ani dovolat do banky ze svého telefonního čísla, aby provedla zablokování karty. Toto se jí podařilo až z druhého telefonního čísla," dodala mluvčí.

Když se žena k účtu konečně dostala, zjistila, že jí pachatel stačil převést peníze ze spořícího účtu na běžný a odtud peníze odcizit převedením na cizí účet. Způsobil jí tak škodu za téměř 200 tisíc korun. Dalších nejméně 120 tisíc korun si podvodník přichystal k převodu, to se mu však již díky blokaci účtu nepodařilo.

Základní rady, jak nenaletět:
Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze.
Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.
Vyzkoušej si www.kybertest.cz a zjisti, kde máš mezery. Buď připraven.

76. Při prodeji dětského kola přišla o 200 tisíc korun

Online ● novinky.cz (Zprávy / Politika) ● 9. 10. 2022, 16:20

Vydavatel: **BORGIS a.s. (cz-00564893)**

Dosah: 1 991 104 ● GRP: 22.12 ● OTS: 0.22 ● AVE: 45000.00 Kč ● Interakcí: 58

Odkaz: https://www.novinky.cz/clanek/krimi-pri-prodeji-detskeho-kola-prisla-o-200-tisic-korun-40411019

Po získání hesel jednal pachatel rychle (ilustrační foto)

Poškozené přišla na WhatsApp zpráva od osoby, vystupující pod jménem Olga, že by měla o kolo zájem. „Ke zprávě pachatel také přiložil odkaz na službu Zásilkovny, přes kterou si prý bude moci utržené peníze vyzvednout a dále uvedl, že poté dorazí kurýr pro zboží," popisovala v neděli mluvčí jihočeské krajské policie Martina Joklová.

„Poškozená přes zaslaný odkaz zadala svůj ID kód a přihlašovací údaje ke svému internetovému bankovnictví. Následně obdržela od banky zprávu o navýšení limitu pro výběr, o který sama nežádala," popisovala dále policejní mluvčí.

„Do bankovnictví se již však nemohla přihlásit, její přihlašovací údaje nefungovaly, nemohla se ani dovolat do banky ze svého telefonního čísla, aby provedla zablokování karty," dodala Joklová.

Nesmějte se obětem podfuku. Dokonce i v IT firmě málem naletěli na falešný e-mail
Bezpečnost

Dovolat se do banky se jí podařilo až z druhého telefonního čísla. „Když se však k účtu konečně dostala, zjistila, že jí pachatel stačil převést peníze ze spořícího účtu na běžný a odtud peníze odcizit převedením na cizí účet, čímž jí způsobil škodu za téměř 200 tisíc korun," konstatovala mluvčí policie.

„Dalších nejméně sto dvacet tisíc korun si podvodník přichystal k převodu, to se mu však již díky blokaci účtu nepodařilo," doplnila Joklová, která upozornila veřejnost k větší obezřetnosti.

Základní rady od policie, jak nenaletět internetovým podvodníkům

- Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.
- Vyzkoušej si **www.kybertest.cz** a zjisti, kde máš mezery. Buď připraven.

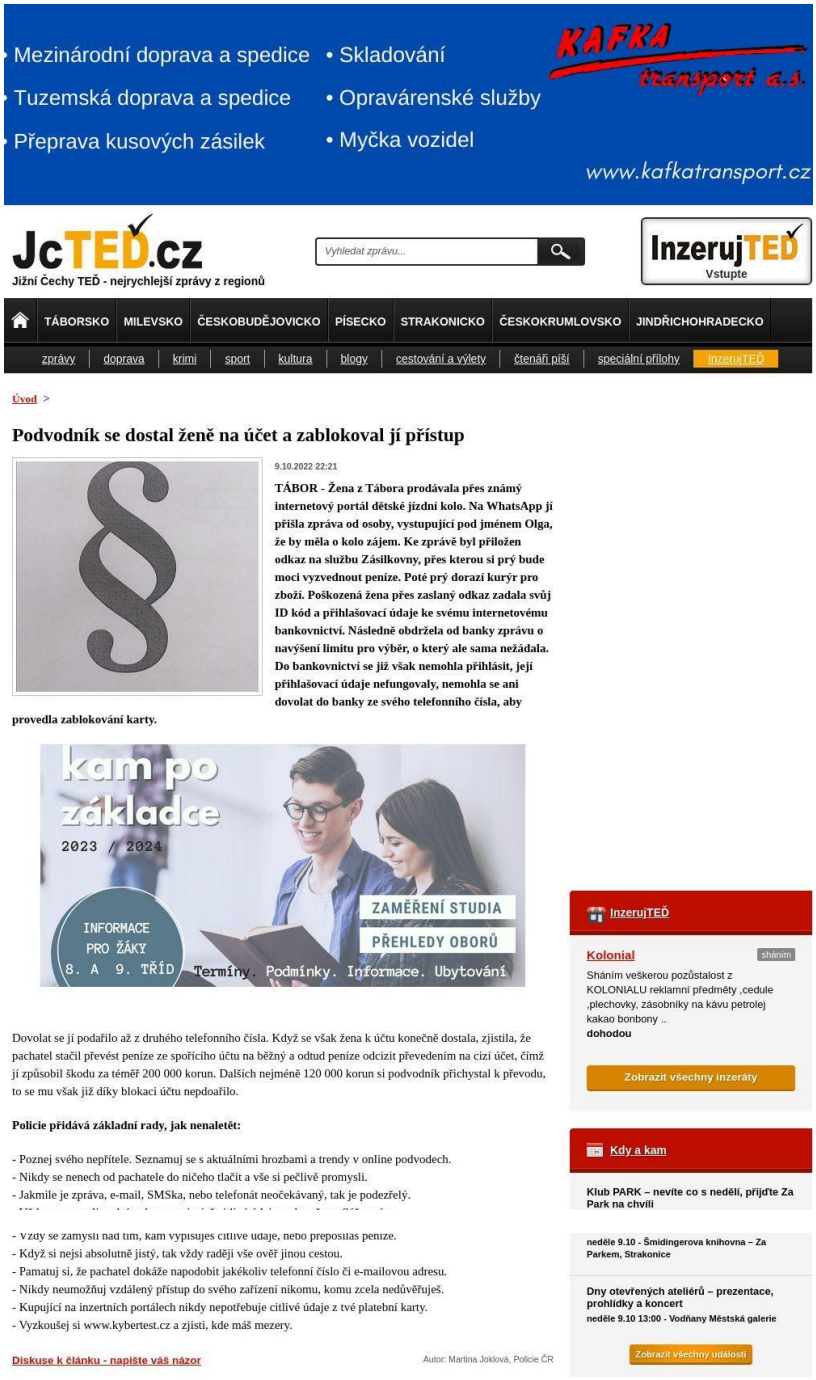
77. Podvodník se dostal ženě na účet a zablokoval jí přístup

Online ● jcted.cz (Regionální zprávy) ● 9. 10. 2022, 22:21

Vydavatel: **Jihočeské týdeníky s.r.o. (cz-26097346)** ● Autor: **Martina Joklová**

Dosah: 7 692 ● GRP: 0.09 ● OTS: 0.00 ● AVE: 13778.71 Kč ● Interakcí: 22

Odkaz: https://www.jcted.cz/68696-podvodnik-se-dostal-zene-na-ucet-a-zablokoval-ji-pristup/

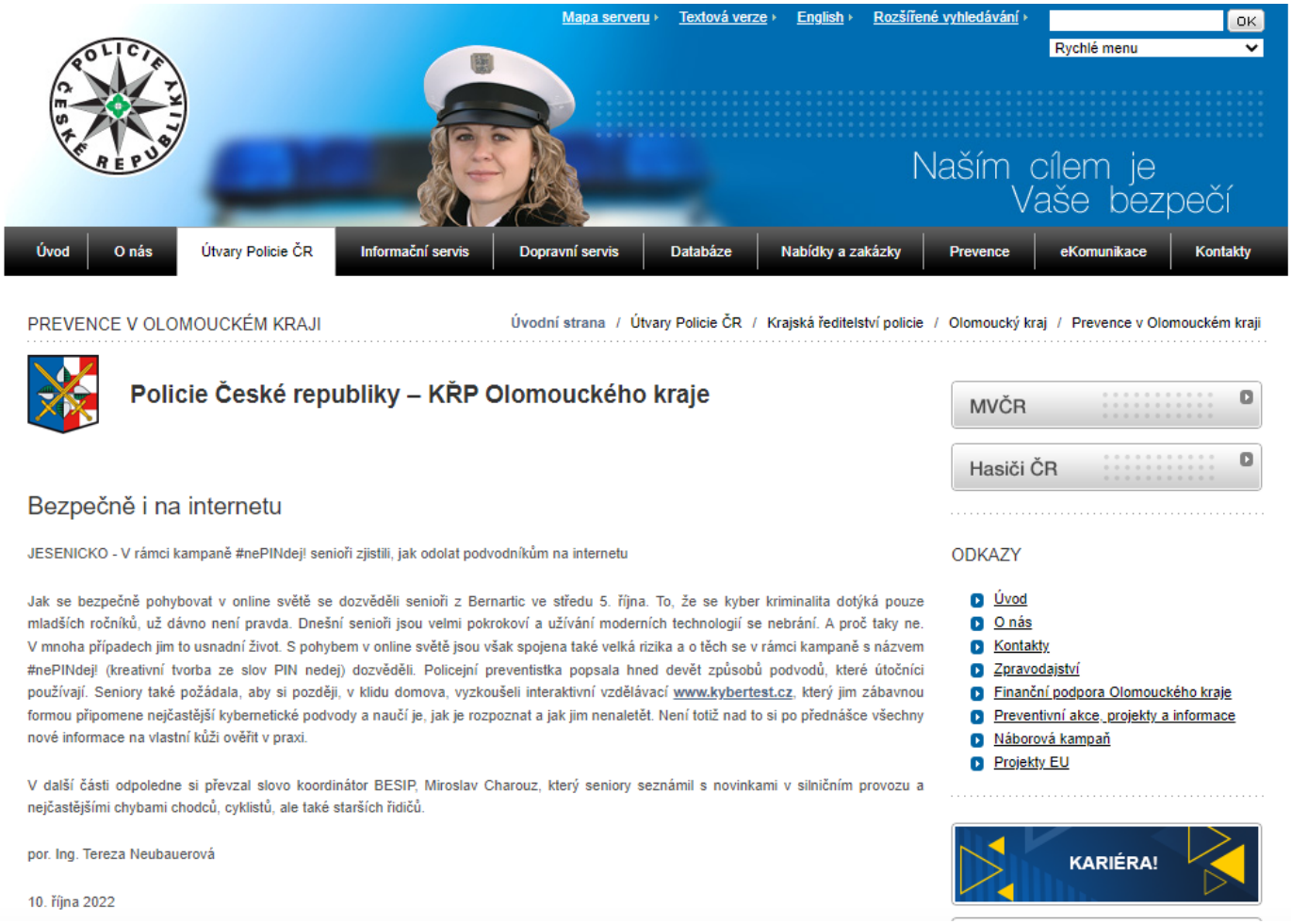


78. Bezpečně i na internetu

Online ● policie.cz (Jiné) ● 10. 10. 2022, 10:45

Dosah: 20 667 ● GRP: 0.23 ● OTS: 0.00 ● AVE: 19996.45 Kč

Odkaz: https://www.policie.cz/clanek/bezpecne-i-na-internetu.aspx



79. Takhle lidem vysají účet. Jak poznat podvod a nepřijít o peníze?

Online ● novinky.cz (Zprávy / Politika) ● 10. 10. 2022, 12:49

Vydavatel: **BORGIS a.s. (cz-00564893)**

Dosah: 1 991 104 ● GRP: 22.12 ● OTS: 0.22 ● AVE: 45000.00 Kč ● Interakcí: 161

Odkaz: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-takhle-lidem-vysaji-ucet-jak-poznat-podvod-a-neprijit-o-penize-40411100

Novinky.cz

Hlavní stránka Stalo se Domácí Volby Zahraniční Válka na Ukrajině Krimi Kultura Ekonomika Finance Sport Žena Vánoce Koktejl
Komentáře Internet a PC AutoMoto Muži Věda a školy Bydlení Cestování Historie Podcasty Speciály Počasí TV program Denní tisk Tiráž

PREZIDENTSKÉ STUDIO | KANDIDÁTI | VOLEBNÍ PRŮZKUMY

Novinky.cz » Internet a PC » Bezpečnost » Takhle lidem vysají účet. Jak poznat podvod a nepřijít o peníze?

Takhle lidem vysají účet. Jak poznat podvod a nepřijít o peníze?

10. 10. 2022, 12:49
Richard Novák, Miloslav Fišer

Z prodeje zboží na internetovém bazaru se stalo nebezpečné dobrodružství. Na prodávající totiž číhají podvodníci, kteří je lstí připraví o peníze. Místo utržených pár stovek za nepotřebné věci tak důvěřivci přijdou klidně i o stovky tisíc korun. Podívejte se, jak útok probíhá a jak se nenechat napálit.

Jeden takový útok zmapoval také uživatel Twitteru vystupující pod jménem NulaPacient, který se útočníkům představil jako Tomáš Pech. Ten vystavil inzerát na Bazoši, načež jej prostřednictvím WhatsAppu kontaktovala žena, která má údajně o zboží zájem.

„Jsem se s vším spokojená a ráda bych si to koupila, ale protože bydlím v Opavě, nemohu si to vyzvednout osobně," stojí v úvodu podvodné zprávy, ve které se odesílatelka či odesílatel snaží zastřešovat přepravní službou DPD.

Prodejci pak útočník tvrdí, že platbu dostanou na účet právě od DPD, pokud se budou řídit zaslaným návodem. Během další komunikace jsou pak z oběti vylákány osobní informace, jako je jméno, e-mailová adresa atp.

Pošlou falešný odkaz

„Hotovo, zaplatila jsem. Zkontrolujte prosím e-mailovou adresu, měli byste obdržet potvrzení objednávky a měli byste obdržet platbu na svůj účet," tvrdí kyberzločinci.

Další průběhy podvodu se pak různí. Někdy skutečně přijde e-mail obsahující odkaz na podvodné stránky, jindy útočníci odkaz zašlou přímo prostřednictvím chatu na WhatsAppu. Na takový odkaz by lidé nicméně nikdy neměli klikat, na stránkách totiž může číhat nějaký škodlivý kód.

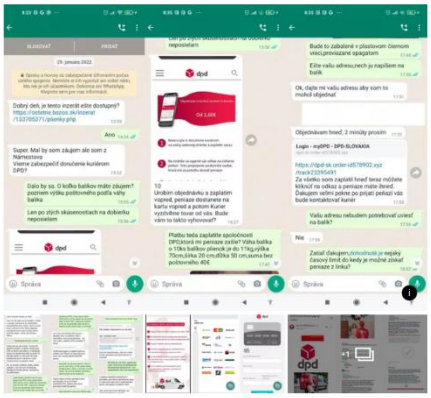
Daleko častěji se ale kyberzločinci prostřednictvím falešné stránky snaží z důvěřivců vylákat údaje k bankovní kartě či přímo k on-line bankovnictví. Prostřednictvím těchto informací pak již snadno vysají z cizího účtu peníze. Lidé by tedy měli především sledovat přesný název zasílané adresy, případně kam směřuje odkaz. Tak zpravidla snadno odhalí, že jim byl zaslán podvodný odkaz.

Žena prodávala dětské oblečení, podvodník ji připravil o 130 tisíc

Krimi

DPD se od podobných podvodů distancovalo již dávno. „Společnost Direct Parcel Distribution nezprostředkovává prodej zboží nebo služeb pro jiné subjekty a nezprostředkovává žádné platební transakce s výjimkou doručení zboží na dobírku a následného odplacení dobírkové částky na účet odesílateli podle jeho pokynů. Nikdy nevyžadujeme zadávání platebních údajů do neautorizovaných zdrojů. Nikdy touto formou nepožadujeme po svých klientech, ať odesílatelích, nebo příjemcích zásilek, čísla platebních karet, kódy CVV apod.," uvedla již dříve přepravní společnost.

Přesto zkušenosti z posledních týdnů jasně ukazují, že někteří důvěřivci se na podobné triky nechají skutečně nachytat. Relativně dobře zvládnutá čeština útočníků totiž přispívá k tomu, že podvody působí poměrně věrohodně. Pokud si lidé nevšimnou špatné webové adresy, která pouze imituje legitimní stránky přepravní společnosti, nemusí být snadné podvod odhalit.



Každý třetí Čech

Česká policie ve spolupráci s antivirovou společností Eset letos v červnu publikovala průzkum, který se zaměřoval na podvodníky na internetových bazarech. Z něj vyplynulo, že 22,64 % dotázaných prodává zboží na webu často a téměř polovina respondentů je alespoň jednou k prodeji zboží využila (48,73 %). Internetové bazary nejčastěji využívají lidé ve věku od 30 do 40 let.

Vlastní zkušenost s podvody na bazarech má 31 % dotázaných, zpravidla jde opět o jedince ve věku od 30 do 40 let. Pozitivní je, že 20,64 % respondentů uvedlo, že včas odhalili podvod a nevznikla jim žádná finanční škoda. Pouze necelá desetina lidí (9,36 %) přiznala, že je podvodníci připravili o méně než 1000 Kč, 5 % dotázaným pak byla způsobena škoda do 5000 Kč.

Podvodníci nejčastěji komunikovali se svými oběťmi přes chatovací aplikaci Messenger (12,27 %), e-mail (10,82 %) či WhatsApp (7,18 %).

„Internetové bazary jsou v poslední době stále populárnější, a bylo proto jen otázkou času, kdy zde kyberkriminalita začne narůstat. Z pohledu bezpečnosti se nejedná o nic nového, techniky používané útočníky jsou známé. To, co je nové, je celkový rozsah těchto aktivit. A výsledky tohoto průzkumu jej bohužel potvrzují," varoval Ondřej Šafář z Esetu.

Základní rady od policie, jak nenaletět internetovým podvodníkům

- Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, esemeska nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.
- Vyzkoušej si www.kybertest.cz a zjisti, kde máš mezery. Buď připraven.

80.Kampaň „Ne-pin-dej“ se snaží seniory upozornit na rizika na internetu

Online ● tvmorava.cz (Regionální zprávy) ● 10. 10. 2022, 13:28

Autor: **Josef Čermák**

Dosah: 333 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 2174.29 Kč

Odkaz: https://www.tvmorava.cz/kampan-ne-pin-dej-se-snazi-seniory-upozornit-na-rizika-na-internetu/

Hlavní strana › Zprávy › Česko

Kampaň „Ne-pin-dej“ se snaží seniory upozornit na rizika na internetu

ZPRÁVY ČESKO OLOMOUCKÝ KRAJ 13:28, 10. října 2022

„Ne-pin-dej“. Ani za milion, zlaté prase, královskou korunu. Myšleno – nikomu nedávej svá hesla, piny k platebním kartám a další přístupové údaje. Touto osobitou kampaní varují policisté veřejnost ve svém projektu proti internetovým podvodníkům. V tomto duchu školili například i seniory v Bernarticích na Jesenicku. V rámci prevence si zájemci vyzkoušeli také interaktivní vzdělávací test. Ten je také volně k dispozici, i podle věkových kategorií, na adrese kybertest.cz.

Textovky z regionu

Pozor na železniční výluku

Výluka se týká trati 30 Drahanovice a 307 Pro Červenka.

prostejov.eu před 3 hodir

Kvíz, autorské čtení prohlídka prostor. Rakouská knihovna slaví třicetiletí

Uplynulo třicet let od z Rakouské knihovny Olo katedře germanistiky F fakulty Univerzity Palac pomyslné dveře otevře

upol.cz před 4 hodinami

Načíst další

81. Podvodníci na Bazoši zruinovali ženě život: vysáli jí z účtu skoro 200 tisíc korun

Online ● chip.cz (IT / Technologie) ● 10. 10. 2022, 14:00

Vydavatel: **Burda International CZ s.r.o. (cz-15273598)** ● Autor: **Jakub Fišer**

Dosah: 17 126 ● GRP: 0.19 ● OTS: 0.00 ● AVE: 20000.00 Kč

Odkaz: https://www.chip.cz/novinky/podvodnici-na-bazosi-zruinovali-zene-zivot-vysali-ji-z-uctu-skoro-200-tisic-korun/

NOVINKY

Podvodníci na Bazoši zruinovali ženě život: vysáli jí z účtu skoro 200 tisíc korun

10.10.2022 14:00 | Jakub Fišer + PŘIDAT KOMENTÁŘ

Neobyčejně zlomyslný podvod na internetovém inzertním portále Bazoš zasáhl ženu z Táborska. Pokoušela se prodat dětské kolo, podvodník z ní ale vylákal údaje k bankovnímu účtu a přišla tak o 200 tisíc korun.

Před podvodníky na internetové inzertní platformě Bazoš jsme již několikrát upozorňovali. Obvykle se snaží působit jako zájemce o zboží, které prodáváte. Ozve se vám tedy, že nabídku přijímá, ale pro zboží se nemůže dostavit – pošle k vám domů tedy kurýra.

Pak vám ještě řekne, že je potřeba zaplatit poštovné, které vám následně proplatí v hotovosti. Samozřejmě, že žádný kurýr nikdy nepřijede a pokud vy sdělíte podvodníkům údaje ke své platební kartě nebo bankovnímu účtu, máte v tu ránu po úsporách. Jako se to stalo ženě v okrese Tábor.

PODVODNÍCI UKRADLI ŽENĚ 200 TISÍC KORUN

Na zmíněném inzertním portále žena prodávala dětské kolo, na WhatsApp se jí pak ozvala zájemkyně Olga. Ke zprávě také podvodník přiložil falešný odkaz na web Zásilkovny, přes kterou si prý bude moci utržené peníze vyzvednout a dále uvedl, že poté dorazí kurýr pro zboží. Tedy naprosto klasický modus operandi.

Jakmile důvěřivá žena sdělila "Olze" údaje k bankovnímu účtu, obdržela od banky prakticky okamžitě SMS zprávu o navýšení limitu pro výběr; ačkoliv sama o něj nežádala. Pak už to šlo ráz na ráz: než stačila účet dočasně zablokovat, pachatel vybral ze spořicího účtu skoro 200 tisíc korun. Dalších nejméně 120 tisíc korun si podvodník přichystal k převodu, to se mu však již díky blokaci účtu nepodařilo, informuje Policie České republiky (PČR) ve své tiskové zprávě.

Na závěr PČR ještě doplňuje seznam základních pouček, kterých byste se měli držet, abyste se vyvarovali podobným podvodům:

- Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Vyzkoušej si **www.kybertest.cz** a zjisti, kde máš mezery. Buď připraven.

Zdroj: **Policie ČR**

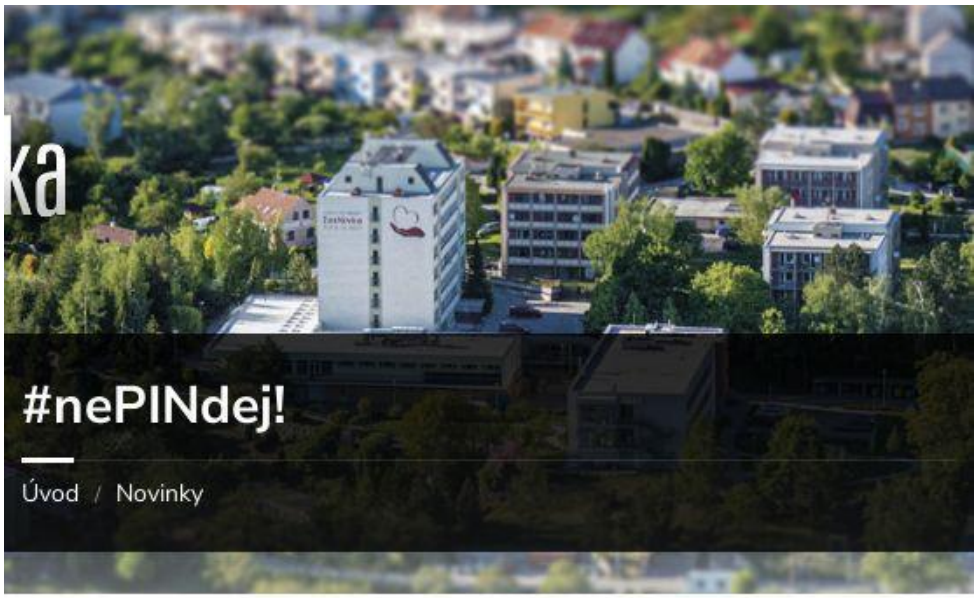
82. #nePINdej!

Online ● zastavka.cz (Regionální zprávy) ● 12. 10. 2022, 17:33

Rubrika: **Novinky**

Dosah: 34 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 860.70 Kč

Odkaz: http://www.zastavka.cz/nepindej/3558/



Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů. Police ČR se připojuje k rozsáhlé vzdělávací

kampani #nePINdej! České bankovní asociace a dalších partnerů, která upozorňuje na sílící nebezpečí podvodů na internetu.

Jak vyplývá z dat České bankovní asociace získaných od jejích členských bank, na jednoho poškozeného klienta připadá průměrná škoda ve výši 161 500 korun. U vishingu, neboli případů podvodného navolávání, jsou částky až čtvrtmilionové.

Klíčovým prvkem kampaně s názvem **#nePINdej!** (kreativní tvorba ze slov PIN nedej) je interaktivní vzdělávací www.kybertest.cz, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim předcházet.

Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. Kybernetická kriminalita již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Kampaň proto cílí na širokou veřejnost počínaje dětmi a mladistvými přes dospělé až na seniory. Otázky v testu jsou tedy generovány dle věku uživatele. Na tvorbě kybertestu se podílela společnost Itego, a.s.
V kybertestu jsou simulovány podvodné SMS, zobrazovací okna k připojení k WIFI sítím, phishingové emaily, zvukové nahrávky podvodných telefonů a mnohé další, tak, aby si je každý uživatel moderních technologií mohl bezpečně vyzkoušet. Testové otázky byly připravovány odborníky na základě reálných případů, jimiž se podvodníci snaží své oběti nachytat.

Pachatelé se při těchto útocích snaží překonávat zejména lidský faktor a pod nejrůznějšími legendami využívají nátlaku, strachu a časové tísně pro záchranu peněz nebo pro realizaci finanční transakce.

Mezi nejčastější podvodné legendy patří:

- **Podvodné navolávání:** Pachatelé se vydávají například za bankéře, policisty, pracovníky technické podpory a snaží se z lidí pod vlivem

strachu vylákat peníze, nebo vzdálený přístup do zařízení oběti, který následně zneužije.

- **Nabídka výhodných investic:** Přesvědčivá lákavá reklama a manipulativní jednání. Cílem pachatele je vylákat z oběti co možná nejvíce finančních prostředků a využívá k tomu přirozenou ziskuchtivost každého z nás.
- **Reverzní inzertní podvody:** Pachatel zareaguje na váš inzerát. Podstrčí vám fiktivní platební bránu, kde vyplníte citlivé bankovní údaje a místo peněz za inzerované zboží přicházíte o všechny úspory.
- **Podvody typu Nigerijské dopisy:** Princip, který funguje už více jak 100 let. Pachatelé sázejí na kvantitu. Vždy se najde někdo, kdo se nechá nachytat na slibovanou cennou zásilku nebo domnělou pomoc. Často zde hraje velkou roli láska.
- **Klasické podvody typu phishing a smishing:** Stále dokonalejší a složitě rozpoznatelné podvodné emaily a SMS nabídky. Na první pohled již nenajdeme podezřelé znaky.

Stále častější praktikou jsou v současné době tzv. reverzní inzertní podvody. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou.

Základní rady, jak nenaletět

- Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.
- Vyzkoušej si www.kybertest.cz a zjisti, kde máš mezery.

83. Falešný e-mail nebo odkaz v SMS. Podvod stojí jednoho člověka desetitisíce

Online ● seznamzpravy.cz (Zprávy / Politika) ● 13. 10. 2022, 17:38

Vydavatel: **Seznam.cz, a.s. (cz-26168685)** ● Autor: **Karolína Štuková**

Dosah: 1 702 492 ● GRP: 18.92 ● OTS: 0.19 ● AVE: 79177.75 Kč ● Interakcí: 67

Odkaz: https://www.seznamzpravy.cz/clanek/tech-technologie-falesny-e-mail-nebo-odkaz-v-sms-podvod-stoji-jednoho-cloveka-desetitisice-216741

Phishingu výrazně přibývá. Ilustrační foto.

17:38

Nečekaný e-mail nebo esemeska, za kterými se skrývá podvod, poškozené uživatele stojí průměrně desítky tisíc korun. Množství těchto podvodů navíc každým rokem narůstá.

Stále častější a dokonalejší. Tak dnes mluví odborníci z oblasti kybernetické bezpečnosti o desetiletí známém digitálním podvodu zvaném phising (vyslovuje se fišink).

I když toto cizí slovo možná neznáte, je velmi pravděpodobné, že jste se s ním už setkali na vlastní kůži.

E-maily, které vyzývají adresáta k zadání osobních údajů na falešné webové stránce, jejíž podoba je takřka identická s tou oficiální, se podle dat společnosti Cisco řadí mezi čtyři nejčastější internetové hrozby. Kromě samotného phishingu jsou na dalším místě neoprávněná těžba kryptoměn na cizím zařízení, trojské koně a ransomware (program, který blokuje počítačový systém nebo šifruje data a za odemknutí požaduje výkupné). Tyto čtyři formy jsou podle Cisca 10krát četnější než ostatní případy kybernetického ohrožení.

Jasnější představě o tom, jak se v dnešní době stále častěji setkáváme s internetovými útoky v podobně phishingu, poslouží čísla v boxu níže:

Phishing v číslech

Celkem **86 %** firem zaznamenalo minimálně jeden pokus uživatele připojit se na phishingový web.

Každý **99.** došlý e-mail obsahuje phishingový útok.

30 % z těchto e-mailů někdo otevře.

90 % všech kyberútoků začíná právě phishingovým e-mailem.

Zdroj: Data Cisco

Ačkoliv jsou čísla vysoká, phishingových útoků každoročně stále přibývá.

„Počet útoků roste každoročně, nicméně akcelerace v posledních dvou letech je způsobena dynamickým rozvojem digitalizace. Roste počet aplikací a veřejnost bere digitální prostředí jako samozřejmou součást života, bohužel stále velké procento veřejnosti není schopno detekovat podvodné jednání, internet skýtá svojí podstatou možnost v krátkém čase atakovat obrovské množství uživatelů a i při nízké míře procentuální úspěšnosti je výdělek oproti nutné investici zajímavý," vysvětlujete Luděk Tichý, manažer specializovaného útvaru ICT bezpečnosti České pošty.

Jak jsou na tom vaše znalosti základních principů bezpečného chování na internetu, si můžete vyzkoušet v online interaktivním kybertestu, který v rámci vzdělávací kampaně spustila Česká bankovní asociace.

Falšované logo a náklady na dopravu balíků

Právě Česká pošta od roku 2018 bojuje v rámci phishingových útoků s rostoucím počtem zneužití jejich loga, které představuje pro veřejnost jistou důvěryhodnost.

„Portfolio našich služeb bohužel vytváří ideální prostředí pro podvodné jednání, zvláště ve spojení s nakupováním po internetu a zasílání zboží, no a v neposlední řadě poskytování peněžních služeb ve spolupráci se státem," popisuje Tichý z České pošty.

ANKETA

Myslíte si, že poznáte podvodný e-mail s phishingem?

Ano

67,1 %

Ne

Ne

32,9 %

Celkem hlasovalo 79 čtenářů.

Z pohledu charakteru podvodu se podle jeho slov nejčastěji jedná o falešné oznámení nedoplatku za poštovní zásilku (balík), kdy se útočník pod záminkou doplatku formou elektronické platby dostane k údajům o platební kartě a obratem oběti konto „vybílí“.

Dalším úspěšným klonem podvrhu je spuštění platební aplikace GooglePay a nebo ApplePay a podvrhem zadání platby na daleko větší částku, než inzeruje, oběť provede platbu na konto útočníka v zahraničí (mimo EU).

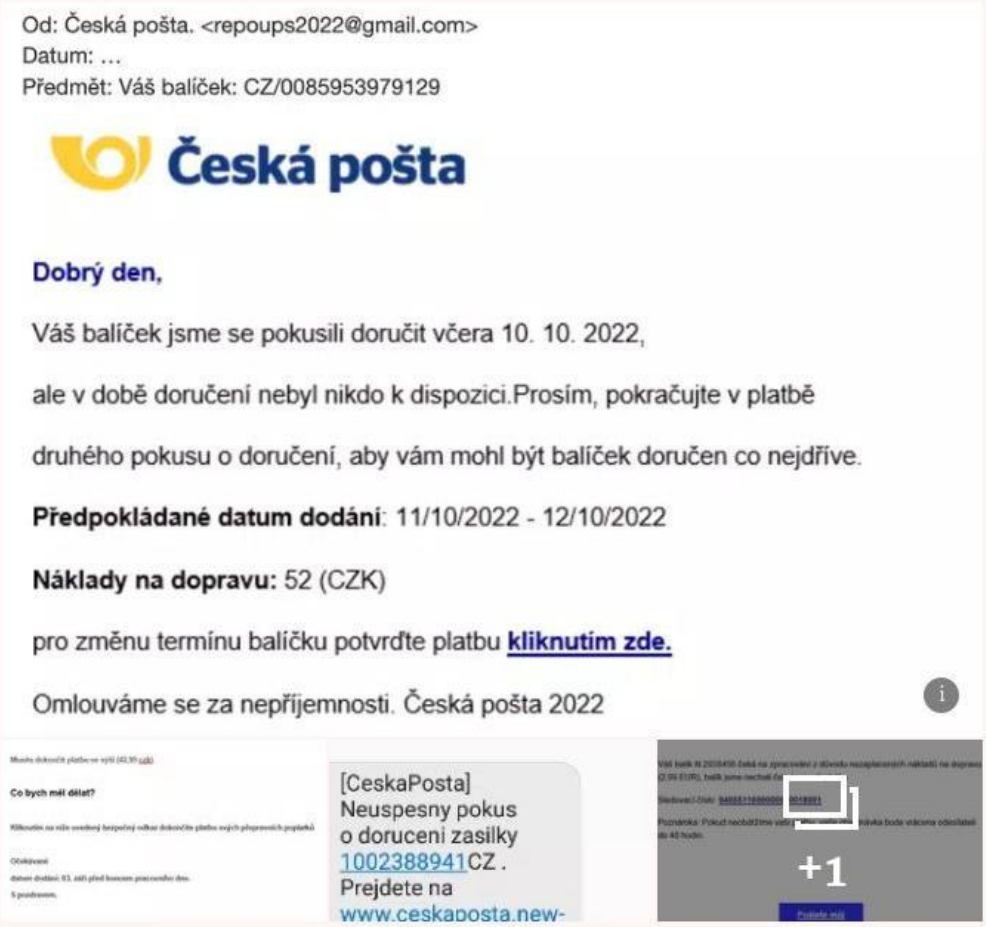
Kyberútoků na banky a jejich klienty přibývá. Jaké jsou typické scénáře

6. 9. 18:33

„Základním verifikačním údajem je číslo balíku, které lze ověřit v aplikaci Pošta on-line, pokud číslo neexistuje, jedná se o podvrh. V poslední době se objevuje i podvrh formou oznámení výplaty přeplatku na dani a snaha vymámit z oběti opět údaje k platební kartě a zaútočit na bankovní účet,“ doplňuje manažer specializovaného útvaru ICT bezpečnosti České pošty.

Rozpoznání tohoto podvodu ale není složité, protože Česká pošta platbu formou on-line karet neprovádí. Nedoplatek na jakékoli službě není možný, protože platbu provádí vždy odesílatel, a pokud se jedná o dobírku,

platí příjemce přímo doručovateli při předání.



O trochu mladší varianta, která se k uživatelům dostává stále častěji, je pak takzvaný SMS phishing. Ten se začal rozšiřovat právě s vývojem smartphonů. Není proto výjimkou, že uživateli přijde například autorizační SMS nebo přihlášení do Apple Pay. I v těchto případech se podvodné zprávy snaží z uživatele vylákat citlivé osobní údaje.

Útok z mailu vlastního šéfa

Další speciální a velmi nebezpečnou formu phishingu představuje takzvaný Business E-mail Compromise (BEC), což je útok cílený na firmy.

Tento druh phishingu je jedním z finančně nejškodlivějších online zločinů.

„Typicky podvodník předstírá, že je např. finančním či generálním ředitelem firmy a v dobře koncipovaném e-mailu zaslaném do finančního oddělení firmy vyjadřuje naléhavou potřebu uhradit fakturu nebo převést peníze," upozorňuje Milan Habrcetl, bezpečnostní expert Cisco.

Velkou komplikací, která dělá tento druh podvodu složitě rozpoznatelný, je fakt, že podvodníci mají pečlivě nastudované detaily z pracovního i soukromého života nadřízeného, a dokážou tak velmi autenticky předstírat, že jsou někým jiným.

„Podvodné e-maily bývají zpravidla odeslány pozdě během dne, často ve čtvrtek nebo pátek nebo před státním svátkem. Časté jsou i případy, kdy například známý dodavatel nebo úřední osoba (např. exekutor) vymáhá uhrazení nějakého poplatku, či dokonce dluhu," doplňuje Habrcetl.

Podle zprávy americké FBI dosahují ztráty z této formy phishingu za rok 2021 více než 40 miliard dolarů (zhruba bilion korun), přičemž mezi lety 2019 a 2021 došlo k nárůstu těchto případů o 65 procent. FBI přitom zároveň udává, že s těmito útoky se setkaly skutečně všechny země na světě.

Tipy, jak se bránit phishingovému útoku ve firmě:

- Důležité finanční pokyny nemají být nikdy zadávány e-mailem, ale například přes informační systém firmy.
- Pokud si nejste jisti, že zpráva opravdu přišla od nadřízeného, hned se mu ozvěte.
- Buďte velmi opatrní na všechny výzvy, které požadují rychlou reakci, vytvářejí dojem vysoké urgentnosti a snaží se vás připravit o čas, abyste si je

nemohli dobře promyslet.

Zdroj: Cisco

S kybernetickými podvody se ale setkávají prakticky veškeré oblasti napojené na internetovou síť. Podle dat Národní centrály proti organizovanému zločinu v Česku bylo do letošního července zachyceno přes deset tisíc trestných činů páchaných v kyberprostoru.

Například podle dat České bankovní asociace zaznamenalo pokus o útok v loňském roce 81 procent bankovních institucí. Na klienty bank jen za prvních sedm měsíců letošního roku směřovalo přes 20 tisíc útoků, za celý rok 2020 to přitom bylo zhruba čtyřikrát méně.

Dramaticky narostly hlavně podvodné telefonáty, tzv. vishing, které patří

„Dramaticky narostly hlavně podvodné telefonáty, tzv. vishing, které patří k těm nejzákeřnějším," popisuje výkonná ředitelka České bankovní asociace Monika Zahálková. Problém je navíc i to, že se zvyšuje úspěšnost útoků.

Téměř každý druhý podvodný telefonát v současné době bohužel končí škodou pro klienta. Průměrná částka, o kterou klienti při phishingových útocích přijdou, se na jednoho klienta pohybuje kolem 73 tisíc korun, ukazují data ČBA.

Tipy pro uživatele, jak se bránit phishingovému útoku:

- Lidé si často myslí, že útočník použije špatnou češtinu nebo že email bude obsahovat zjevné gramatické chyby. Není to tak, dnešní phishingové útoky jsou psány velmi kvalitně.
- Email může přijít na první pohled od někoho známého, jméno v hlavičce mailu se dá zfalšovat a emailová adresa odesílatele také. Pozor tedy na zprávy s neobvyklými výzvami, které jsou na první pohled od známého člověka (například – „potřebuji pomoc, klikni na tuto stránku a vyplň tam údaje")
- Adresa pro kliknutí může v mailu vypadat neškodně – když na ni najedete myší, ukáže se skutečná adresa, kam byste se proklikli. Pokud neodpovídá adrese napsané v textu, může být nebezpečná. Útočníci také umí webové adresy různě zřetězit, takže se nakonec ocitnete na úplně jiné stránce, než na jakou jste klikli.
- Na internetu jsme si zvykli, že „bezpečné" webové stránky mají v adrese „HTTPS:" Nicméně i útočníci si mohou založit web s tímto zabezpečením.
- Nikdy nesdělujte osobní nebo finanční údaje nikomu mailem.

Zdroj: Cisco

84. Vzdělávací kampaň #nePINdej!

Online ● brno-stred.cz (Regionální zprávy) ● 14. 10. 2022, 14:21

Dosah: 3 911 ● GRP: 0.04 ● OTS: 0.00 ● AVE: 10379.83 Kč

Odkaz: https://www.brno-stred.cz/aktuality/vzdelavaci-kampan-nepindej~n15951

iční úřad na nové adrese Nádražní 4. Úřední dny jsou pondělí a středa, 8.00–17.00 hodin.

Úřad MČ | Potřebuji si vyřídit | Poradna | Mohlo by vás zajímat | Další | Kontakty

ň #nePINdej!

14. října 2022

Vzdělávací kampaň #nePINdej!

Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů. Police ČR se připojuje k rozsáhlé vzdělávací kampani #nePINdej! České bankovní asociace a dalších partnerů, která upozorňuje na sílící nebezpečí podvodů na internetu.

Jak vyplývá z dat České bankovní asociace získaných od jejích členských bank, na jednoho poškozeného klienta připadá průměrná škoda ve výši 161 500 korun. U vishingu, neboli případů podvodného navolávání, jsou částky až čtvrtmilionové. Klíčovým prvkem kampaně s názvem #nePINdej! (kreativní tvorba ze slov PIN nedej) je interaktivní vzdělávací www.kybertest.cz, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim předcházet.

Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. Kybernetická kriminalita již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Kampaň proto cílí na širokou veřejnost počínaje dětmi a mladistvými přes dospělé až na seniory. Otázky v testu jsou tedy generovány dle věku uživatele. Na tvorbě kybertestu se podílela společnost Itego, a. s. V kybertestu jsou simulovány podvodné SMS, zobrazovací okna k připojení k WIFI sítím, phishingové emaily, zvukové nahrávky podvodných telefonů a mnohé další tak, aby si je každý uživatel moderních technologií mohl bezpečně vyzkoušet. Testové otázky byly připravovány odborníky na základě reálných případů, jimiž se podvodníci snaží své oběti nachytat.

Pachatelé se při těchto útocích snaží překonávat zejména lidský faktor a pod nejrůznějšími

Pachatelé se při těchto útocích snaží překonávat zejména lidský faktor a pod nejrůznějšími legendami využívají nátlaku, strachu a časové tísně pro záchranu peněz nebo pro realizaci finanční transakce.

Mezi nejčastější podvodné legendy patří:

1. Podvodné navolávání:
Pachatelé se vydávají například za bankéře, policisty, pracovníky technické podpory a snaží se z lidí pod vlivem strachu vylákat peníze, nebo vzdálený přístup do zařízení oběti, který následně zneužije.
2. Nabídka výhodných investic:
Přesvědčivá lákavá reklama a manipulativní jednání. Cílem pachatele je vylákat z oběti co možná nejvíce finančních prostředků a využívá k tomu přirozenou ziskuchtivost každého z nás.
3. Reverzní inzertní podvody:
Pachatel zareaguje na váš inzerát. Podstrčí vám fiktivní platební bránu, kde vyplníte citlivé bankovní údaje a místo peněz za inzerované zboží přicházíte o všechny úspory.
4. Podvody typu Nigerijské dopisy:
Princip, který funguje už více jak 100 let. Pachatelé sázejí na kvantitu. Vždy se najde někdo, kdo se nechá nachytat na slibovanou cennou zásilku nebo domnělou pomoc. Často zde hraje velkou roli láska.
5. Klasické podvody typu phishing a smishing:
Stále dokonalejší a složitě rozpoznatelné podvodné emaily a SMS nabídky. Na první pohled již nenajdeme podezřelé znaky.

Stále častější praktikou jsou v současné době tzv. reverzní inzertní podvody. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu "bezpečnou platbu", tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou.

Základní rady, jak nenaletět:

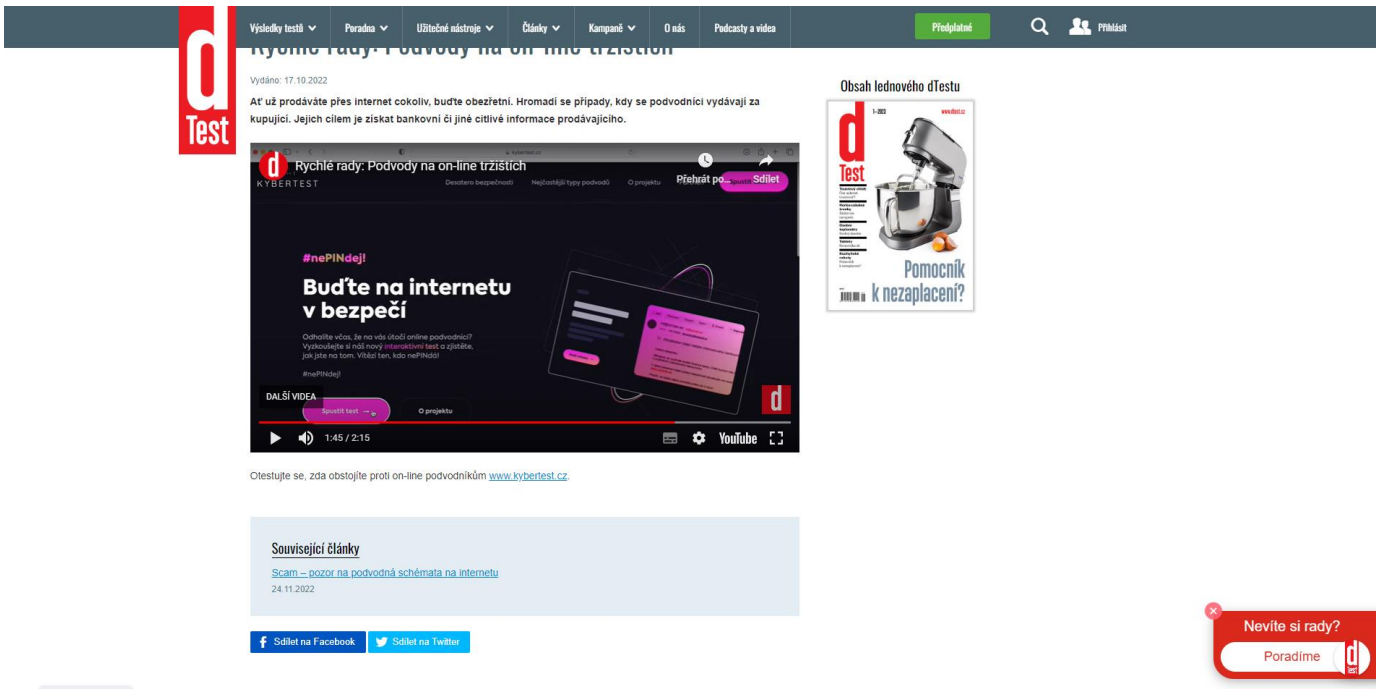
- Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v on-line podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv telefonní číslo či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.

85. Rychlé rady: Podvody na on-line tržištích

Online ● dtest.cz (Jiné) ● 17. 10. 2022, 11:23

Dosah: 17 404 ● GRP: 0.19 ● OTS: 0.00 ● AVE: 7332.92 Kč

Odkaz: https://www.dtest.cz/clanek-9791/rychle-rady-podvody-na-on-line-trzistich



86.Okresní lumpárny a karamboly uplynulých dní

Online ● jesenickenoviny.cz (Regionální zprávy) ● 17. 10. 2022, 11:27

Vydavatel: **Jiří Fanta (cz-65120167)** ● Rubrika: **Aktuální zprávy**

Dosah: 105 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 1445.29 Kč

Odkaz: https://www.jesenickenoviny.cz/?p=27100

Okresní lumpárny a karamboly uplynulých dní

17.10.2022 Aktuální zprávy, Hříšní lidé... žádné komentáře

Jak bezpečně v online světě

Jak se bezpečně pohybovat v online světě se dozvěděli senioři z Bernartic ve středu 5. října. To, že se kyber kriminalita dotýká pouze mladších ročníků, už dávno není pravda. Dnešní senioři jsou velmi pokrokoví a užívání modernich technologií se nebrání. A proč taky ne. V mnoha případech jim to usnadní život. S pohybem v online světě jsou však spojena také velká rizika a o těch se v rámci kampaně s názvem #nePINdej! (kreativní tvorba ze slov PIN nedej) dozvěděli. Policejní preventistka popsala hned devět způsobů podvodů, které útočníci používají. Seniory také požádala, aby si později, v klidu domova, vyzkoušeli interaktivní vzdělávací www.kybertest.cz, který jim zábavnou formou připomene nejčastější kybernetické podvody a naučí je, jak je rozpoznat a jak jim nenaletět. Není totiž nad to si po přednášce všechny nové informace na vlastní kůži ověřit v praxi.

V další části odpoledne si převzal slovo koordinátor BESIP, Miroslav Charouz, který seniory seznámil s novinkami v silničním provozu a nejčastějšími chybami chodců, cyklistů, ale také starších řidičů.

Prodávala ledničku, podvodník ji připravil o téměř 30 000 korun

Ve čtvrtek 6. října se na policisty obrátila 28letá žena z Jeseníku s tím, že se stala obětí podvodu. Téhož dne dopoledne ji kontaktoval zájemce, který reagoval na inzerát, ve kterém nabízela prodej ledničky. Nabídku zveřejnila jak na sociální síti, tak i na inzertním portále. Kupující se nabídl, že zařídí dopravu i platbu přes kurýrní společnost. Poté ženě zaslal odkaz, po jehož odkliknutí byla přesměrována na internetové stránky, na kterých vyplnila číslo své platební karty, dobu platnosti i třímístný kód. Následně se jí zobrazily webové stránky její banky, na kterých vyplnila přihlašovací údaje do internetového bankovnictví. Krátce nato zjistila, že z jí z konta zmizelo téměř 30 000 korun.

Policisté případ prověřují pro podezření ze spáchání přečinu podvodu. V případě dopadení, prokázání viny a odsouzení hrozí pachateli trest odnětí svobody až na dvě léta, zákaz činnosti nebo propadnutí věci.

Apelujeme na občany, aby nikdy neklikali na přijaté neznámé odkazy a v žádném případě nevyplňovali, či nesdělovali údaje ke své platební kartě, či internetovému bankovnictví!

Falešný bankéř připravil seniora o téměř 300 000 korun

Začátkem října přijal 66letý muž z Jesenicka telefonát od údajného pracovníka centrální banky, který jej informoval o napadení bankovního účtu. Současně se mu nabídl, že mu bude nápomocen při ochraně jeho financí. Volající muži poradil, aby si na počítači nainstaloval program, kterým si zabezpečí svůj účet. Muž postupoval podle jeho pokynů, avšak celá akce nakonec ztroskotala v momentě, kdy došlo na zadávání údajů pro přihlášení do internetového bankovnictví. Muž jej totiž neměl vůbec zřízeno. Podvodník si ovšem i v takový moment věděl rady. Důvěřivce navedl přímo do banky s pokynem, aby si vybral finanční prostředky, které měl odeslat na chráněné účty. Jejich čísla mu záhy zaslal. V obavách o své finance si dotyčný nejprve zablokoval platební karty a poté zamířil do své banky. U přepážky zadal dvě transakce, kterými nechal ze svého konta odeslat na požadované účty finanční prostředky v celkové výši téměř 300 000 korun.

Včerejšího dne se opět dostavil do své banky pro nové platební karty. Mimo jiné se bankovní pracovnici svěřil s celým příběhem. Ta mu sdělila, že se stal pravděpodobně obětí podvodu a ať neprodleně kontaktuje policisty.

Kriminalisté případ prověřují pro podezření ze spáchání přečinu podvodu, na který trestní zákoník ukládá trest odnětí svobody na jeden rok až pět let nebo peněžitý trest.

Nereagujte na telefonní hovory, SMS zprávy a e-maily, ve kterých se Vás někdo pokouší vmanipulovat do situace, že jsou Vaše finanční prostředky v ohrožení a Vy musíte udělat další kroky pro jejich záchranu. Kdyby byly Vaše peníze v ohrožení, tak banka již sama zareaguje a učiní další potřebná opatření. V případě pochybností vždy kontaktujte svou banku, a pokud Vás shora naznačeným způsobem již někdo kontaktoval, neváhejte se obrátit na tísňovou linku Policie České republiky.

87. ČBA News, číslo 21/2022; str. 3

Tisk ● ČBA News; str. 3 (Ekonomika / Finance / Právo) ● 18. 10. 2022

Odkaz: náhled

Počet online podvodů neustále roste. Jen za poslední dva roky se zvýšil čtyřnásobně. Podvodníci si přitom své cíle vybírají napříč všemi generacemi, bez rozdílu věku či vzdělání. Česká bankovní asociace proto spustila v rámci své celonárodní kampaně #nePINdej! interaktivní online kvíz – www.kyberhra.cz, který je obdobou oblíbeného Kybertestu, ale obsahuje otázky vhodné pro žáky druhého stupně základních škol, středních škol, odborných učilišť a víceletých gymnázií. Kyberhru si mohou vyzkoušet mladiství jak jednotlivě, tak i hromadně, například v rámci třídy či školy. *„Letošní rok jsme pojali jako testovací. Chceme školám ukázat, že mají možnost Kyberhru využít ve svých výukových programech a žáky a studenty tak seznámit prostřednictvím reálných ukázek, ale zároveň formou hry, s nebezpečími, která na ně v kyberprostoru číhají. V příštím roce pak plánujeme zvýšit motivaci škol vyzkoušet si Kyberhru vyhlášením soutěže o ceny,"* doplnila Andrea Machálková, gestorka finančního vzdělávání veřejnosti České bankovní asociace.
Kampaň #nePINdej!, jejíž součástí je i zmíněná Kyberhra, zcela jistě patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly doposud realizovány. Unikátní je i to, že se do ní zapojily jak orgány státní správy, které se kyberbezpečností zabývají, tak klíčové firmy českého byznysu. Kromě České bankovní asociace, která je realizátorem projektu, jsou do kampaně zapojeny Policie České republiky, Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), itego, a.s., CISCO, Thein

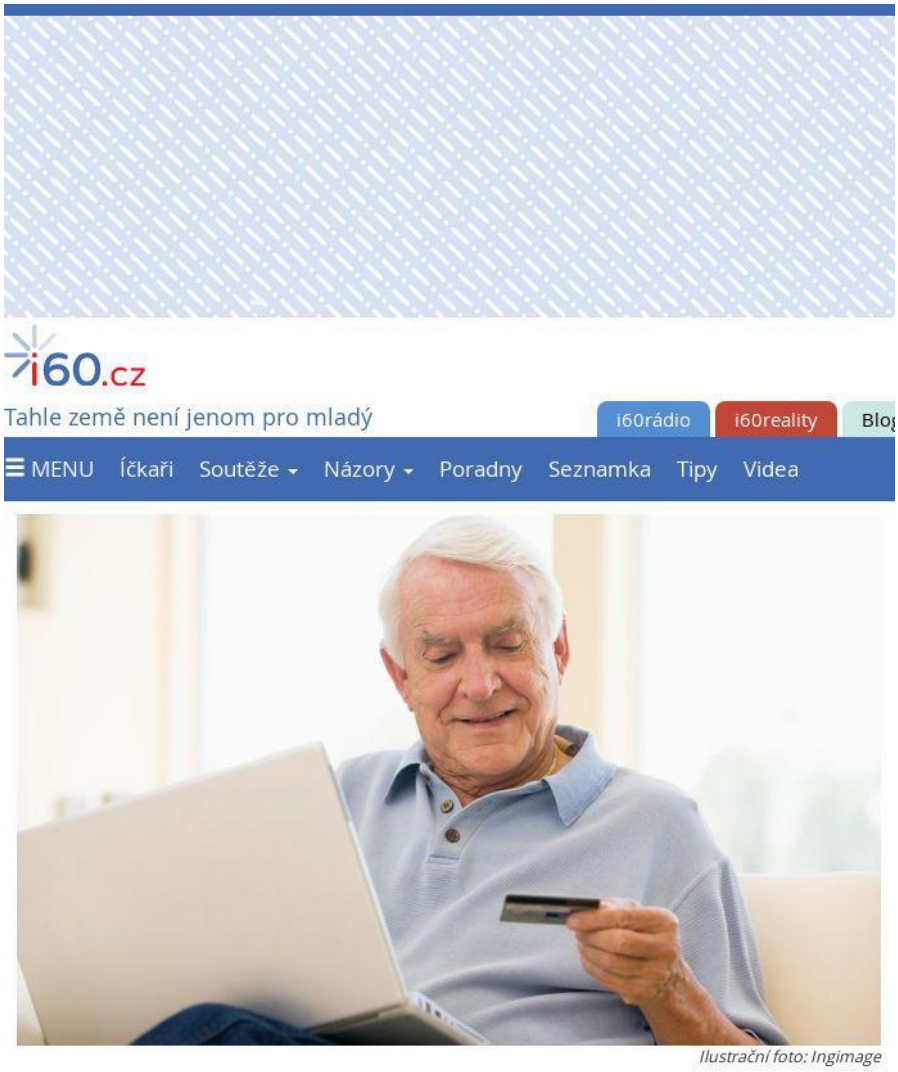
88. Jak odhalit phishing

Online ● i60.cz (Jiné) ● 18. 10. 2022, 6:47

Vydavatel: **i60 Publishers, s.r.o. (cz-24214868)**

Dosah: 16 724 ● GRP: 0.19 ● OTS: 0.00 ● AVE: 18532.40 Kč

Odkaz: https://www.i60.cz/clanek/detail/31276/jak-odhalit-phishing



Ilustrační foto: Ingimage

Jak odhalit phishing

18. 10. 2022

Phishing (vyslovováno: fišing) je útok, který se pokouší ukrást vaše peníze tím, že napadeného přiměje odhalit osobní údaje, například čísla kreditních karet, bankovní údaje nebo hesla. Internetoví zločinci přitom předstírají, že jsou renomované společnosti, přátelé nebo vaši známí.

Kybernetičtí podvodníci se při pokusech vás okrást neustále zdokonalují. K vašim penězům se již dávno nesnaží dostat jen s pomocí e-mailů slibujících snové dědictví či falešných stránek plných gramatických chyb a překlepů. Jejich metody jsou stále sofistikovanější a kombinují nedostatečné zabezpečení vašich chytrých telefonů a PC, znalost vašich osobních dat, umění manipulace a moment překvapení.

Útočníci v podvodných e-mailech chtějí, abyste udělali něco, co po vás nikdy žádná spolehlivá obchodní společnost či banka prostřednictvím nevyžádaného e-mailu nebude požadovat: zadání údajů o platební kartě nebo hesel k internetovému bankovnictví, stáhnutí souboru zaslaného v příloze apod.

Jak odhalit phishing?

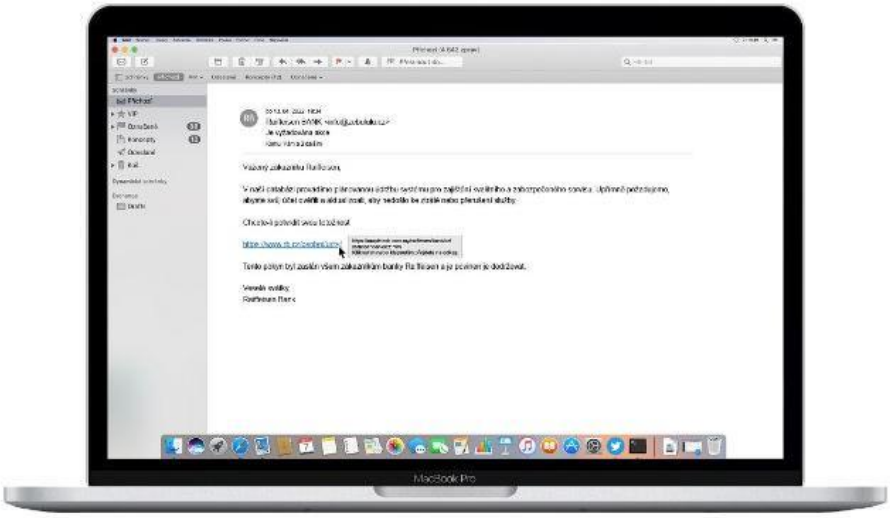
Kyberločinci používaj řadu způsobů, jak vás oklamat. Varováním pro vás mohou být tyto situace:

- **Naléhavá výzva**. Pokud obdržíte e-mail, který vás vyzývá k okamžitému kliknutí, volání nebo otevření přílohy, mějte se na pozoru. Právě vytváření falešné naléhavosti je běžným trikem phishingových útoků a podvodů.
- **Pravopisné chyby a špatná gramatika**. Pokud je e-mailová zpráva plná očividných pravopisných nebo gramatických chyb, může se jednat o podvod. Tyto chyby jsou někdy výsledkem neobratného překladu z cizího jazyka a někdy jsou záměrné ve snaze vyhnout se filtrům, které se snaží tyto útoky blokovat.
- **Neznámé jméno**. Pokud dostanete e-mail od někoho, koho nepoznáváte, nebo kterého outlook identifikuje jako nového odesílatele, věnujte chvíli pečlivému prozkoumání zprávy, než budete pokračovat. Dost často jde právě o phishing.
- **Chybné domény**. Pokud e-mail tvrdí, že pochází od renomované společnosti, jako je Microsoft nebo vaše banka, ale e-mail se odesílá z jiné e-mailové domény, jako je Gmail.com, nebo microsoftsupport.ru je to pravděpodobně podvod. Dávejte si také dobrý pozor na drobné změny v legitimním názvu domény. Jako například micros0ft.com, kde je druhé „o“ nahrazené znakem 0, nebo rnicrosoft.com, kde je písmeno „m“ nahrazené písmeny „r“ a „n“. Jedná se o běžné podvodnické triky.
- **Podezřelé odkazy a přlohy**. Pokud jsou v e-mailu nebo ve zprávě na sociálních sítích odkazy a přílohy, musíte být opatrní. Často můžete být nuceni z různých důvodů kliknout na odkaz nebo stáhnout a otevřít přílohu. Tyto přílohy však mohou sloužit k maskování virů nebo malwaru, které po stažení nebo otevření mohou vést buď ke ztrátě osobních údajů, nebo k instalaci škodlivého softwaru do počítače nebo telefonu. I pouhé kliknutí na ně může infikovat vaše zařízení. Ke stránkám se přihlašujte pouze přímo v prohlížeči, nebo aplikaci, nikdy

prostřednictvím odkazu nebo přílohy zaslané v e-mailu. Pokud máte pochybnosti, kontaktujte klientské centrum instituce, která vám e-mail poslala.

Phishing přes e-mail

Útočníci v podvodných e-mailech chtějí, abyste udělali něco, co po vás nikdy žádná spolehlivá obchodní společnost či autorita prostřednictvím nevyžádaného e-mailu nebude požadovat: zadání údajů o platební kartě nebo hesel k internetovému bankovnictví, stáhnutí souboru zaslaného v příloze apod. Takový podvodný e-mail může vypadat takto:



Phishing přes sociální sítě

Phishingové útoky prostřednictvím sociálních sítí jsou velmi podobné těm uskutečněným prostřednictvím e-mailu. I zde útočníci využívají metod sociálního inženýrství, aby ze svých obětí podvodně vylákali peníze nebo jejich citlivé osobní údaje. Nejčastěji vnikne útočník do profilu oběti na sociální síti a zneužije ho k rozeslání zpráv s podvrženým odkazem jejím přátelům. Útočník často ani nemusí do profilu proniknout, ale jednoduše profil zkopíruje a přátelům z adresáře odešle zprávu, která vypadá, jako by byla odeslána z pravého profilu. Zpráva často obsahuje žádost o peníze, nebo podvodné linky na webové stránky, jejichž prostřednictvím se z vás útočník snaží vylákat citlivé údaje.

Phishing přes sociální sítě může vypadat takto:

Jak se proti phishingu bránit?

Důležitá je obezřetnost. Řiďte se výše uvedenými pravidly v případě, že se vám zdá příchozí e-mail podezřelý. Pokud se vám nezdá, že e-mail přišel například od banky, u níž máte založen osobní účet, neváhejte se obrátit na vašeho osobního bankéře. V případě, že jste už někomu odeslali údaje např. ze své platební karty, nechce si kartu zablokovat, případně se obraťte na Policii České republiky. A rozhodně mějte na svých elektronických zařízeních nainstalován aktualizovaný antivirový program a spamový filtr.

„Obezřetnost je na místě také při řešení pracovních záležitostí. Velmi nebezpečný je takzvaný Business email compromise. Podvodník se vydává například za finančního nebo generálního ředitele a ve věrohodně vypadajícím e-mailu zaslaném z podvržené adresy nařizuje urgentní úhradu faktury nebo převod peněz z firemního účtu," popisuje další z podvodných technik Milan Habrcetl, bezpečnostní expert společnosti Cisco, která je partnerem projektu #nePINdej! – celonárodní vzdělávací kampaně v oblasti kyberbezpečnosti,kterou připravila Česká bankovní asociace.

Součástí tohoto projektu je mimo jiné Kybertest, ve kterém se můžete sami otestovat, zda jste schopni odolat phishingu:

89. Prodávala dětské botičky

Online ● policie.cz (Jiné) ● 18. 10. 2022, 9:33

Dosah: 20 667 ● GRP: 0.23 ● OTS: 0.00 ● AVE: 19996.45 Kč

Odkaz: https://www.policie.cz/clanek/prodavala-detske-boticky.aspx

ZPRAVODAJSTVÍ

Úvodní strana / Útvary Policie ČR / Krajská ředitelst

Policie České republiky – KŘP Královéhradeckého kraje

Prodávala dětské botičky

RYCHNOVSKO – Místo výdělku 250 korun přišla téměř o 70 tisíc.

Za částku 250 korun prodávala 39letá žena z Rychnovska prostřednictvím internetového prodejního portálu dětské botičky. O boty projevil zájem dosud nezjištěný pachatel, vydávající se za ženu, který prodávající kontaktoval prostřednictvím sms zprávy. Následný scénář byl totožný, o jakých jsme vás již v minulosti informovali. Podvodník vyžadoval odeslání cestou kurýrní služby, s čímž poškozená souhlasila. Přes obdržený odkaz vyplnila údaje ke své platební kartě a během chvíle přišla postupně o téměř 70 tisíc korun.

Rychnovští policisté ve věci zahájili úkony trestního řízení pro podezření ze spáchání přečinu podvod, za který hrozí pachateli, v případě odsouzení, trest odnětí svobody až na dvě léta.

Pamatujte!

- Nikdy neklikejte na neznámé odkazy.
- **Nevyplňujte údaje k Vaší osobě, bankovnímu účtu nebo platební kartě v odkazech zaslaných neznámou osobou.**

Základní rady, jak nenaletět

- Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.
- Vyzkoušej si **www.kybertest.cz** a zjisti, kde máš mezery. Buď připraven.

por. Ing. Eliška Pospíšilová
18.10.2022, 9:40

E-mailem Vytisknout

90. Podvodníci nadále okrádají důvěřivé klienty bank. Jak se bránit?

Online ● hyperfinance.cz (Ekonomika / Finance / Právo) ● 19. 10. 2022, 0:00

Dosah: 335 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 2905.51 Kč

Odkaz: https://www.hyperfinance.cz/magazin/podvodnici-nadale-okradaji-duverive-klienty-bank--jak-se-branit/

Hyperfinance.cz
portál pro vaše finance

Půjčky | Účty | Pojištění | Hypotéky | Magazín | Odpovědi | K

Podvodníci nadále okrádají důvěřivé klienty bank. Jak se bránit?

Lenka Rutteová Publikováno 19.10.2022 Aktualita | Banky

Počet útoků na bankovní účty běžných lidí neustále roste. Rok 2022 je navíc ve znamení extrémního nárůstu jak samotného počtu pokusů o útok na peníze uložené v bance, tak skokového růstu v počtu těch úspěšných. Přitom mají jedno společné: oběti útočníkům zcela dobrovolně odevzdaly všechny údaje, které podvodníci k dokončení krádeže potřebují. Ale co s tím? Stačilo by jediné: držet se nového hesla vyhlášeného ČBA: #nePINdej!

Počet online podvodů se za poslední dva roky mnohonásobně zvýšil

Česká bankovní asociace ve spolupráci s Policií ČR pravidelně zveřejňují statistiky týkající se online podvodů a dalších útoků na klienty bank, resp. na jejich běžné účty. A jak to vypadá,

podvodníci si dobře všimli dvou hlavních nedostatků českých bankovních klientů:

- **na běžných účtech drží spoustu peněz (i statisíce)** - místo toho, aby je převedli na spořicí účet, který bude od běžného účtu a jeho platební karty zcela oddělen
- **věří kdekomu a o své platební kartě nebo svém přístupu do online bankovnictví sdělí kdeco a hlavně kdekoliv, případně zašlou kamkoliv.**

Není proto divu, že se Češi coby klienti bank stávají stále oblíbenějšími cíli útoků. *„V loňském se roce se skrze tento typ podvodů na internetu ztratila miliarda korun. Letos se stejná částka ztratila za pouhého půl roku,"* vyčíslil pro server idnes.cz Petr Barák, expert České bankovní asociace na oblast bezpečnosti. Povzbudivá nejsou ani čísla týkající se samotného počtu útoků. Posuďte sami:

- rok 2020: **5 235 útoků**
- rok 2021: **12 239 útoků**
- leden až červenec 2022: **20 660 útoků**

O kolik Češi přicházejí? O dlouholeté úspory. Během pár vteřin

Průměrná škoda, která podvedeným lidem vznikne, byla v červenci 2022 až neuvěřitelných 161 500 Kč. U vishingových podvodů (telefonáty) bývá škoda podle informací serveru měšec.cz v průměru ještě vyšší, 250 000 Kč. U phishingu (e-maily a zprávy na sociálních sítích) je pak škoda v průměru na cca 73 000 Kč.

Jak podvody probíhají? Útočníci si vyžádají všechny údaje, které potřebují

„Podvody jsou postavené na schématu, že klient musí osobně údaje dát a potvrdit. Není to tak, že by útočník vlezl do účtu sám. Dva a půl roku běží kampaň, která klienty upozorňuje na to, aby si dali pozor, jaké údaje a kam zadávají," zájemce o informace ještě upozornil Barák. Sami se tak stáváme spolustrůjci našeho vlastního okradení.

Podvody v online bazarech: pro příjem platby přece nemusí kupující vědět o vaší kartě vůbec nic!

Stále častěji se ke slovu dostávají podvodníci, kteří se rozhodli okrádat prodávající na online

bazarech. Tvrdí jim totiž, že aby mohla být příjemci připsána platba, **musí příjemce zadat o své platební kartě úplně všechno**. Včetně PIN nebo bezpečnostního kódu (na zadní straně karty).

Ale jak upozorňuje Barák: *„Je důležité si uvědomit, jaké údaje po vás chtějí. PIN, CVC kód atd. nemáte nikomu dávat. Není důvod, aby někdo, kdo vám má poslat peníze, chtěl tyto údaje. Důležité je číst také notifikace, které vám během všech transakcí posílá banka*". Ta totiž někdy upozorní, že se děje něco nekalého, ale klient i tak celý proces schválí.

Zavedl vás email opravdu do online bankovnictví? Poznáte to velmi snadno!

Dalšími nástroji podvodníků jsou webové stránky, které mají simulovat, že po kliknutí na podstrčený odkaz jste se přenesli **online bankovnictví vaší banky**. Ve skutečnosti jste ale na stránkách vytvořených podvodníky za účelem přečtení všech vašich údajů sloužících pro vstup do banky a obsluhu účtu.

Jenže jak poznáte, zda jste u své banky a v bezpečí? Je to naštěstí celkem snadné: ve webové adrese musí být základní doména banky (například **kb.cz, csob.cz, mbank.cz, airbank.cz, maxbanka.eu** apod.). Jakmile jsou v adresovém řádku naprosto cizí adresy, které mají banku jen jako součást domény cizího státu, rychle pryč.

> Správné adresy internetového bankovnictví výše uvedených bank jsou následující:
>
> - https://www.kb.cz/cs/obcane/vitejte/internetove-bankovnictvi
> - https://www.csob.cz/portal/lide/ucty/internetove-a-mobilni-bankovnictvi/internetove-bankovnictvi
> - https://www.mbank.cz/osobni/internetove-bankovnictvi/
> - https://ib.airbank.cz/
> - https://www.maxbanka.eu/internetove-bankovnictvi

Kyberhra a celonárodní kampaň ČBA s názvem #nePINdej!

Jak informovala ČBA ve svém newsletteru, v rámci své celonárodní kampaně #nePINdej! spustila interaktivní online kvíz – www.kyberhra.cz, který je obdobou již dobře známého Kybertestu. Ovčem kyberhra obsahuje otázky vhodné pro žáky druhého stupně základních škol, středních škol, odborných učilišť a víceletých gymnázií.

Kampaň #nePINdej!, jejíž součástí Kyberhra je, patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti, které byly dosud v České republice realizovány. Zapojily se jak **orgány**

kyberbezpečnosti, které byly doposud v České republice realizovány. Zapojily se jak **orgány státní správy, které se kyberbezpečností zabývají, tak významné české firmy**:

- Policie České republiky
- Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)
- itego, a.s.
- CISCO
- Thein Security
- Česká pošta
- ČEZ
- Mastercard
- O2
- České dráhy.

Mediálními partnery jsou Česká televize (hlavní mediální partner), Seznam Zprávy, Deník a Cinestar. A jak název projektu vznikl? Jde o kouzelné propojení jak slovesa v negativně vyjádřeném rozkazovacím způsobu, tak tří samostatných slov NE, PIN a DEJ. Zkrátka: PIN nikomu nedávej(te)!

Zdroje: ČBA NEWS 21/2022 / měšec.cz / iDnes.cz

Autor článku:

Lenka Rutteová

Vystudovala Ekonomicko správní fakultu Univerzity Pardubice a doktorské studium na Ekonomické fakultě VŠB-TU v Ostravě. Více

91. IT Podvod

Online ● policie.cz (Jiné) ● 21. 10. 2022, 11:24

Dosah: 20 667 ● GRP: 0.23 ● OTS: 0.00 ● AVE: 19996.45 Kč

Odkaz: https://www.policie.cz/clanek/it-podvod.aspx

ZPRAVODAJSTVÍ

Úvodní strana / Útvary Policie ČR / Krajská ře

Policie České republiky – KŘP Jihočeského kraje

IT Podvod

Táborsko – Chtěl prodat přes inzertní internetový portál přilbu za 500 korun, přišel o statisíce.

Na táborské policisty se obrátila muž ve středním věku a oznámil jim, že v uplynulých dnech ho přes komunikaci v aplikaci WhatsApp kontaktoval domnělý kupec přilby v hodnotě 500 korun, kterou poškozený nabízel k prodeji na jednom z inzertních portálů. Při komunikaci mu kupující zaslal zprávu s hypertextovým odkazem, která jej přesměrovala na stránky kurýrní služby DPD a následně na poškozeným zvolenou banku, kde vyplnil identifikační údaje ke svému bankovnímu účetnictví. Následně zjistil, že ho dosud neznámý pachatel připravil o téměř 300 tisíc korun.

Táborští kriminalisté případ šetří jako přečiny podvod a neoprávněné opatření, padělání a pozměnění platebního prostředku.

Základní rady, jak nenaletět:

- Poznejte svého nepřítele. Seznamujte se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenechte od pachatele do ničeho tlačit a vše si pečlivě promyslete.
- Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamyslete nad tím, kam vypisujete citlivé údaje, nebo přeposíláte peníze.
- Když si nejste absolutně jistí, tak vždy raději vše ověřte jinou cestou.
- Pamatujte si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
- Nikdy neumožňujte vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřujete.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z vaší platební karty.
- Nesdělujte své osobní údaje.
- Nezasílejte ofocené osobní doklady.
- Nesdělujte tištěné informace z platební karty.
- Nesdělujte kód, kterým by vzdáleně přistupoval k vašemu počítači.
- Nesdělujte bankovní autorizační SMS kódy.
- Cizí osobě nikdy neautorizujte platbu.
- V počítači mějte nainstalovaný stále aktualizovaný antivirový program.
- V internetovém bankovnictví mějte nastaveny co nejnižší limity a zvyšujte je jen na aktuální potřebu zaplacení konkrétní platby.

Vyzkoušejte si www.kybertest.cz a zjistěte, kde máte mezery.

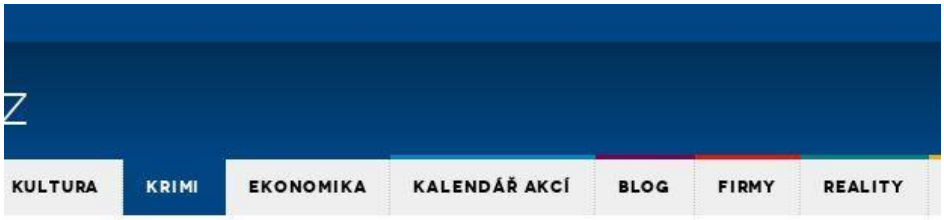
por. Bc. Lenka Pokorná ta.pis@pcr.cz

92. IT Podvod

Online ● regionjih.cz (Regionální zprávy) ● 21. 10. 2022, 11:24

Dosah: 34 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 860.70 Kč

Odkaz: https://www.regionjih.cz/zpravodajstvi/it-podvod-180031/



IT Podvod

Táborsko – Chtěl prodat přes inzertní internetový portál přilbu za 500 korun, přišel o statisíce.

Na táborské policisty se obrátila muž ve středním věku a oznámil jim, že v uplynulých dnech ho přes komunikaci v aplikaci WhatsApp kontaktoval domnělý kupec přilby v hodnotě 500 korun, kterou poškozený nabízel k prodeji na jednom z inzertních portálů. Při komunikaci mu kupující zaslal zprávu s hypertextovým odkazem, která jej přesměrovala na stránky kurýrní služby DPD a následně na poškozeným zvolenou banku, kde vyplnil identifikační údaje ke svému bankovnímu účetnictví. Následně zjistil, že ho dosud neznámý pachatel připravil o téměř 300 tisíc korun. Táborští kriminalisté případ šetří jako přečiny podvod a neoprávněné opatření, padělání a pozměnění platebního prostředku. Základní rady, jak nenaletět: Poznejte svého nepřítele. Seznamujte se s aktuálními hrozbami a trendy v online podvodech. Nikdy se nenechte od pachatele do ničeho tlačit a vše si pečlivě promyslete. Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý. Vždy se zamyslete nad tím, kam vypisujete citlivé údaje, nebo přeposíláte peníze. Když si nejste absolutně jisti, tak vždy raději vše ověřte jinou cestou. Pamatujte si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu. Nikdy neumožňujte vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřujete. Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z vaší platební karty. Nesdělujte své osobní údaje. Nezasílejte ofocené osobní doklady. Nesdělujte tištěné informace z platební karty. Nesdělujte kód, kterým by vzdáleně přistupoval k vašemu počítači. Nesdělujte bankovní autorizační SMS kódy. Cizí osobě nikdy neautorizujte platbu. V počítači mějte nainstalovaný stále aktualizovaný antivirový program. V internetovém bankovnictví mějte nastaveny co nejnižší limity a zvyšujte je jen na aktuální potřebu zaplacení konkrétní platby. Vyzkoušejte si www.kybertest.cz a zjistěte, kde máte mezery. por. Bc. Lenka Pokorná ta.pis@pcr.cz tisková mluvčí a preventistka 21. října 2022

93. Další oběť IT podvodu je z Tábora. Chtěl prodat přilbu, přišel o tři sta tisíc

Online ● taborsky.denik.cz (Regionální zprávy) ● 21. 10. 2022, 12:28

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)** ● Autor: **Zuzana Gabajová** ● Rubrika: **Zprávy**

Dosah: 3 756 ● GRP: 0.04 ● OTS: 0.00 ● AVE: 10197.34 Kč ● Interakcí: 23

Odkaz: https://taborsky.denik.cz/zlociny-a-soudy/dalsi-obet-it-podvodu-je-z-tabora-chtel-prodat-prilbu-prisel-o-tri-sta-tisic-202.html

Další oběť IT podvodu je z Tábora. Chtěl prodat přilbu, přišel o tři sta tisíc

DNES 12:28

Zuzana Gabajová
Editorka
Napište mi

Řady obětí internetových podvodů rozšířil muž z Tábora, který zadal na falešnou stránku přihlašovací údaje ke svému bankovnímu účtu a přišel o statisíce korun.

"Na táborské policisty se obrátil muž ve středním věku s tím, že v uplynulých dnech ho přes komunikaci v aplikaci WhatsApp kontaktoval domnělý kupec přilby v hodnotě pět set korun, kterou poškozený nabízel k prodeji na jednom z inzertních portálů," přiblížila policejní mluvčí Lenka Pokorná. "Při komunikaci mu kupující zaslal zprávu s hypertextovým odkazem, která jej přesměrovala na stránky kurýrní služby DPD a následně na poškozeným zvolenou banku, kde vyplnil identifikační údaje ke svému bankovnímu účetnictví. Následně zjistil, že ho dosud neznámý pachatel připravil o téměř 300 tisíc korun."

Podvodníci dál na jihu Čech bílí lidem účty. Oběti jim samy posílají přístupy

PŘEČÍST ČLÁNEK ›

Táborští kriminalisté případ šetří jako přečiny podvod a neoprávněné opatření, padělání a pozměnění platebního prostředku a znovu varují občany, aby byli před obezřetní.

A jak nenaletět? Policie má tyto rady:
•Poznejte svého nepřítele. Seznamujte se s aktuálními hrozbami a trendy v online podvodech.
•Nikdy se nenechte od pachatele do ničeho tlačit a vše si pečlivě promyslete.
•Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
•Vždy se zamyslete nad tím, kam vypisujete citlivé údaje, nebo přeposíláte peníze.
•Když si nejste absolutně jisti, tak vždy raději vše ověřte jinou cestou.
•Pamatujte si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
•Nikdy neumožňujte vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřujete.
•Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z vaší platební karty.
•Nesdělujte své osobní údaje.
•Nezasílejte ofocené osobní doklady.
•Nesdělujte tištěné informace z platební karty.
•Nesdělujte kód, kterým by vzdáleně přistupoval k vašemu počítači.
•Nesdělujte bankovní autorizační SMS kódy.
•Cizí osobě nikdy neautorizujte platbu.
•V počítači mějte nainstalovaný stále aktualizovaný antivirový program.
•V internetovém bankovnictví mějte nastaveny co nejnižší limity a zvyšujte je jen na aktuální potřebu zaplacení konkrétní platby.

Vyzkoušejte si **www.kybertest.cz** a zjistěte, kde máte mezery.

94. Chtěl prodat přilbu a přišel o statisíce. Stal se obětí internetového podvodu

Online ● budejcka.drbna.cz (Regionální zprávy) ● 22. 10. 2022, 10:51

Vydavatel: **TRIMA NEWS s.r.o. (cz-26081890)** ● Autor: **František Linduška**

Dosah: 6 476 ● GRP: 0.07 ● OTS: 0.00 ● AVE: 17913.09 Kč ● Interakcí: 31

Odkaz: https://budejcka.drbna.cz/krimi/36461-chtel-prodat-prilbu-a-prisel-o-statisice-muz-se-stal-obeti-jednoho-z-internetovych-podvodu.html

Chtěl prodat přilbu a přišel o statisíce. Stal se obětí internetového podvodu

Dnes, 10:51

Jihočeští kriminalisté vyšetřují další dva případy internetových podvodů, kterých navzdory četným varováním policistů neustále přibývá. V jednom z nich dokonce podvodník obral muže prodávajícího svou přilbu o téměř tři sta tisíc korun.

Hned dvěma novými případy internetového podvodu se zabývají jihočeští kriminalisté. Na konci tohoto týdne se jim přihlásil muž středního věku z Táborska s tím, že jej falešný zájemce obral o téměř tři sta tisíc korun při internetovém prodeji použité přilby na kolo.

„Poškozený chtěl na jednom z inzertních internetových portálů prodat přilbu v hodnotě pěti set korun. Domnělý kupec jej kontaktoval přes mobilní aplikaci WhatsApp a při komunikaci mu zaslal zprávu s hypertextovým odkazem,“ uvedla policejní mluvčí **Lenka Pokorná**. Odkaz prodávajícího zavedl na falešné stránky jedné z kurýrních služeb, kde nic netušící muž vyplnil požadované údaje ke své platební kartě. Záhy poté ale zjistil, že mu falešný zájemce z konta vybral skoro tři sta tisíc korun.

K podobnému incidentu došlo i v Českém Krumlově, nicméně škoda, kterou falešný zájemce o inzerát na portálu bazoš.cz způsobil, byla v tomto případě výrazně nižší. Pod záminkou koupě dřevěného roštu na postel navázal podvodník opět přes aplikaci WhatsApp kontakt s prodávajícím a v konverzaci mu zaslal odkaz na stránku jednoho z dopravců. *„Na této stránce poškozený jako ve všech podobných případech vyplnil údaje o své platební kartě včetně bezpečnostního kódu. S těmito informacemi už pak podvodníkovi nic nebránilo v tom, aby poškozeného obral o více než 24 tisíc korun,“* informoval policejní mluvčí **Miroslav Šupík** s tím, že českokrumlovští policisté nyní po pachateli usilovně pátrají. V případě dopadení a prokázání viny dotyčnému hrozí až dvouletý pobyt za mřížemi.

Policisté na podobné internetové podvody veřejnost dlouhodobě upozorňují a varují před nebezpečnými transakcemi, zejména při internetových prodejích. Všechny případy mají společné to, že pachatel z poškozeného různými způsoby, nejčastěji právě přes podvodnou stránku dopravce, vylákají údaje k platební kartě, ze které mu následně vybere veškeré finanční prostředky. Pachatelé také v některých případech mohou napodobit číslo banky nebo dokonce policie.

„Je potřeba si uvědomit, že když něco prodáváte, kupující nepotřebuje znát číslo vaší platební karty a už vůbec ne její platnost či bezpečnostní kód. Odkaz na stránky dopravce je tedy vždy falešný a jeho cílem je získat od vás potřebné informace, které následně poslouží k vykradení účtu,“ upozornil Šupík.

Policisté na svém webu nabízejí několik rad a tipů, jak podobným internetovým podvodníkům snadno nenaletět. Některé z nich najdete dole pod článkem. Zároveň si na stránkách kybertest.cz můžete otestovat své znalosti v oblasti kyberbezpečnosti.

Základní rady, jak nenaletět internetovému podvnodníkovi:

- Poznejte svého nepřítele. Seznamujte se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenechte od pachatele do ničeho tlačit a vše si pečlivě promyslete.
- Jakmile je zpráva, e-mail, SMS, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamyslete nad tím, kam vypisujete citlivé údaje, nebo přeposíláte peníze.
- Když si nejste absolutně jisti, tak vždy raději vše ověřte jinou cestou.
- Pamatujte si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
- Nikdy neumožňujte vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřujete.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z vaší platební karty.
- Nesdělujte své osobní údaje.
- Nezasílejte ofocené osobní doklady.
- Nesdělujte tištěné informace z platební karty.
- Nesdělujte kód, kterým by vzdáleně přistupoval k vašemu počítači.
- Nesdělujte bankovní autorizační SMS kódy.
- Cizí osobě nikdy neautorizujte platbu.
- V počítači mějte nainstalovaný stále aktualizovaný antivirový program.
- V internetovém bankovnictví mějte nastaveny co nejnižší limity a zvyšujte je jen na aktuální potřebu zaplacení konkrétní platby.

95. Přišli o 1,7 milionu i statisíce z půjčky. Policie ukázala, jak podvodníci obírají důvěřivce

Online ● novinky.cz (Zprávy / Politika) ● 23. 10. 2022, 11:44

Vydavatel: **BORGIS a.s. (cz-00564893)**

Dosah: 1 991 104 ● GRP: 22.12 ● OTS: 0.22 ● AVE: 45000.00 Kč ● Interakcí: 317

Odkaz: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-oskubou-lidi-o-penize-ktere-ani-nemaji-policie-ukazala-jak-pracuji-podvodnici-40412430

Ilustrační foto

Různé internetové podvody plní policejní statistiky bohužel stále častěji, a to napříč celou republikou. Mluvčí policie Lenka Drahokoupilová popsala hned několik případů z tohoto týdne, které se udály na Znojemsku.

„Největší způsobená škoda v případech oznámených v průběhu týdne je 1,7 milionu korun. Tolik peněz vylákal falešný námořník od šedesátileté ženy, která s ním zhruba rok komunikovala přes sociální sítě," prohlásila Drahokoupilová.

Podle ní je evidentní, že domnělý námořník postupoval velmi sofistikovaně. „Poslal jí balík z Austrálie a potom prý přicestuje i on – virtuální nápadník. Zamilovaná žena všemu věřila a posílala peníze na složité a komplikované doručení zásilky. Zatím se nedočkala balíčku a ani milovaného muže," podotkla policejní mluvčí.

Falešný bankéř připravil seniora na Jesenicku o téměř 300 tisíc korun
Bezpečnost

V jednom z dalších případů hrál klíčovou roli bankéř, který však – jak se později ukázalo – byl falešný. Podvedl pětatřicetiletou ženu, kterou připravil o statisíce korun.

„Kontaktoval ji po telefonu a sdělil, že si předchozí den zažádala z jejího účtu o úvěr jiná žena. Potom jí popsal prý jedinou možnost, jak o peníze nepřijít. Ať si ve svém internetovém bankovnictví zažádá o co největší možný úvěr, který následně bance ihned vrátí tak, že peníze vloží přes zaslaný QR kód do bitcoinmatu," popsala průběh podvodu Drahokoupilová.

Žena bohužel tvrzení uvěřila a postupovala přesně podle instrukcí. „Na vlastní žádost dostala úvěr ve výši 326 tisíc korun, peníze vybrala v bance ve Znojmě a hotovost pak vložila do bitcoinmatu u hraničního přechodu Hatě.

Podvodníci cílí na žadatele o příspěvky
Bezpečnost

Podvody na bazarech stále vychází

Přestože policie i bezpečnostní experti pravidelně varují před podvody na internetových bazarech, útočníkům se stále daří důvěřivce oklamat. Na vlastní kůži se o tom v tomto týdnu přesvědčila čtyřiačtyřicetiletá žena, která chtěla prodat již nepotřebnou dětskou pistoli.

„Na internetu zveřejnila inzerát a neznámý zájemce jí poslal odkaz na dopravce. Ona vyplnila veškeré údaje k platební kartě i internetovému bankovnictví a následně zjistila, že jí na účtu chybí 24 tisíc korun," uvedla policejní mluvčí.

Jak přes kopírák probíhal prodej topného žebříku, za který se snažila utržit 400 korun pětatřicetiletá žena ze Znojemska. „Neznámý zájemce zareagoval na její inzerát na internetovém portálu a zaslal jí odkaz na webovou stránku dopravce. Vyplnila všechny údaje ke své platební kartě a během pár minut jí z účtu zmizelo téměř padesát tisíc korun," řekla Drahokoupilová.

„Všemi případy se intenzívně zabýváme a po zatím neznámých internetových podvodnících pátráme. Zároveň také občany upozorňujeme, aby byli ostražití a nikomu citlivé údaje ke svým financím nedávali," uzavřela policejní mluvčí.

Prodávám jednu blbost na bazoši a konečně se ozvala i DPD podvodnice.
pic.twitter.com/iReMu3Rcps
— Široko (@NulaPacient) October 8, 2022

Takto vypadá komunikace s podvodníkem z internetového bazaru.

Každý třetí Čech

Česká policie ve spolupráci s antivirovou společností Eset letos v červnu publikovala průzkum, který se zaměřoval na podvodníky na internetových bazarech. Z něj vyplynulo, že 22,64 % dotázaných prodává zboží na webu často a téměř polovina respondentů je alespoň jednou k prodeji zboží využila (48,73 %). Internetové bazary nejčastěji využívají lidé ve věku od 30 do 40 let.

Vlastní zkušenost s podvody na bazarech má 31 % dotázaných, zpravidla jde opět o jedince ve věku od 30 do 40 let. Pozitivní je, že 20,64 % respondentů uvedlo, že včas odhalili podvod a nevznikla jim žádná finanční škoda. Pouze necelá desetina lidí (9,36 %) přiznala, že je podvodníci připravili o méně než 1000 Kč, 5 % dotázaným pak byla způsobena škoda do 5000 Kč.

Podvodníci nejčastěji komunikovali se svými oběťmi přes chatovací aplikaci Messenger (12,27 %), e-mail (10,82 %) či WhatsApp (7,18 %).

„Internetové bazary jsou v poslední době stále populárnější, a bylo proto jen otázkou času, kdy zde kyberkriminalita začne narůstat. Z pohledu bezpečnosti se nejedná o nic nového, techniky používané útočníky jsou známé. To, co je nové, je celkový rozsah těchto aktivit. A výsledky tohoto průzkumu jej bohužel potvrzují," varoval Ondřej Šafář z Esetu.

Základní rady od policie, jak nenaletět internetovým podvodníkům

- Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech

- Pozřej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, esemeska nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.
- Vyzkoušej si **www.kybertest.cz** a zjisti, kde máš mezery. Buď připraven.

Podvod ani nenahlásí

Alarmující je zjištění, že bezprostředně – tedy do 24 hodin – nahlásilo podvod pouze 4,09 % dotázaných, 20,82 % respondentů nenahlásilo podvodné jednání policii vůbec, 7 % lidí se snažilo s podvodníky nejprve komunikovat, následně se obrátili na policii.

„Jsme si vědomi toho, že jen část obětí nás osloví s tím, že byla podvedena. Ale i v této skupině vidíme značný nárůst. Z toho důvodu chceme společně s bezpečnostní komunitou na toto téma opětovně upozornit, protože jednoznačně vidíme, že edukace je jedním z hlavních způsobů ochrany," vysvětlila Zuzana Pidrmanová, vedoucí oddělení prevence Policejního prezidia České republiky.

Podobné podvody mají často stejný scénář – podvodník nejprve přiměje prodávajícího skrze různé argumenty k tomu, aby vyplnil osobní údaje i informace z platební karty na podvodnou stránku, která vypadá legitimně.

Dva miliony zmizely za hodinu a půl. Další lidé naletěli podvodníkům
Bezpečnost

„Tímto způsobem je pachatel schopen z účtu odcizit všechny finanční prostředky, protože mu oběť dobrovolně sdělí veškeré přístupy ke své platební kartě nebo do internetového bankovnictví, zároveň si může vzít na jméno poškozené osoby i předem schválený úvěr," varovala Pidrmanová.

Lidé by tedy měli být při prodeji na internetových bazarech velmi obezřetní. „Podvodníci často využívají prvky tzv. sociálního inženýrství, pomocí kterých se během komunikace snaží vzbudit důvěru protistrany. O zboží mají zájem a chtěli by jej co nejdříve. Naléhají. Jedním z aktuálních trendů je, že se vás osoba na druhé straně snaží přesvědčit, že vše uhradila, posílá pro vyzvednutí zboží přepravce a vám zbývá jen potvrdit bankovní údaje na webové stránce, která je ale podvržená," uzavřel Šafář.

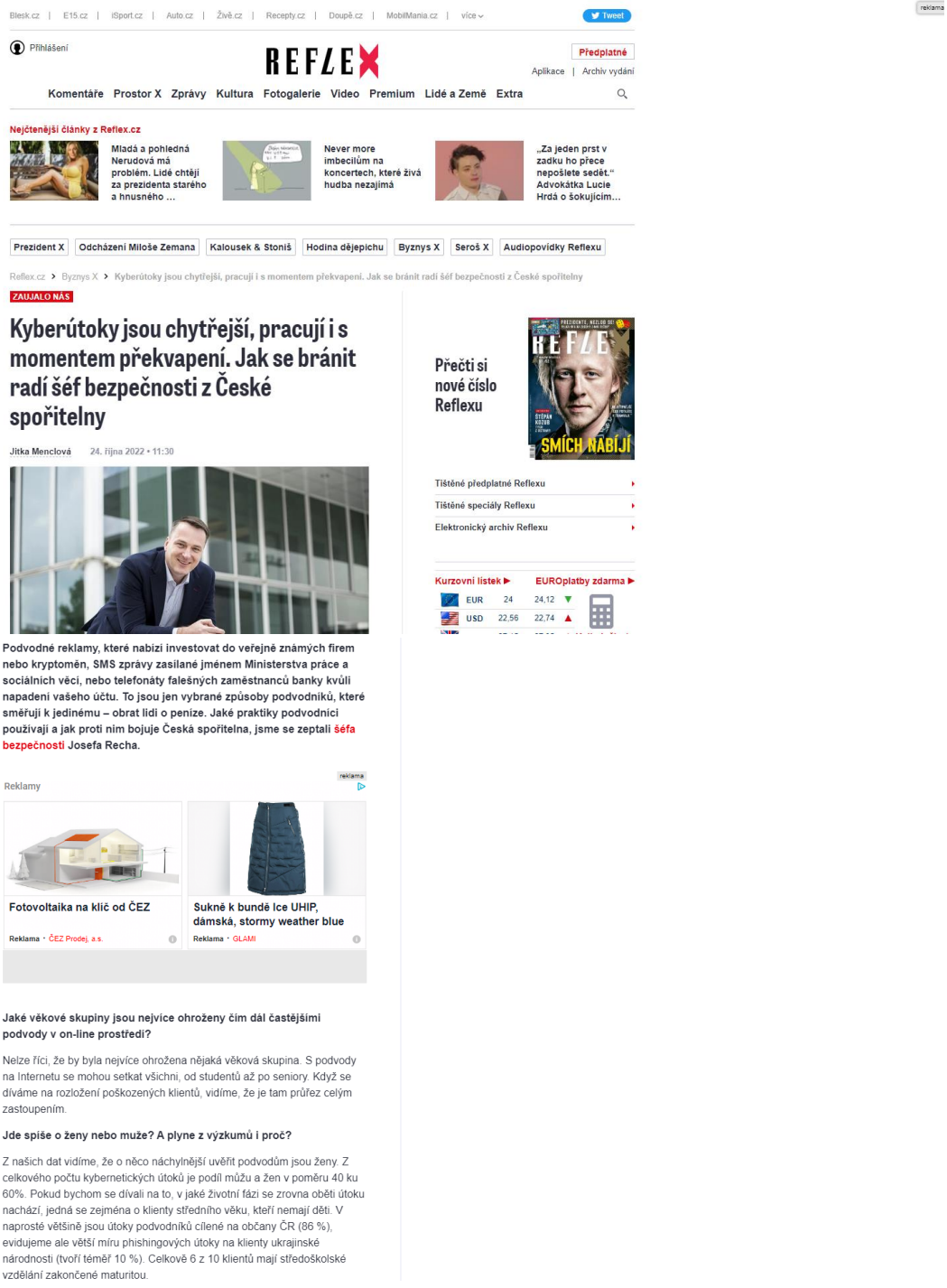
96. Kyberútoky jsou chytřejší, pracují i s momentem překvapení. Jak se bránit radí šéf bezpečnosti z České spořitelny

Online ● reflex.cz (Společenské) ● 24. 10. 2022, 11:30

Vydavatel: **CZECH NEWS CENTER a.s. (cz-02346826)** ● Autor: **Jitka Menclová**

Dosah: 62 776 ● GRP: 0.70 ● OTS: 0.01 ● AVE: 20000.00 Kč

Odkaz: https://www.reflex.cz/clanek/byznys-x/115738/kyberutoky-jsou-chytrejsi-pracuji-i-s-momentem-prekvapeni-jak-se-branit-radi-sef-bezpecnosti-z-ceske-sporitelny.html



Blesk.cz | E15.cz | iSport.cz | Auto.cz | Živě.cz | Recepty.cz | Doupě.cz | MobilMania.cz | více

Tweet

Přihlášení

REFLEX

Předplatné

Aplikace | Archiv vydání

Komentáře Prostor X Zprávy Kultura Fotogalerie Video Premium Lidé a Země Extra

Nejčtenější články z Reflex.cz

Mladá a pohledná Nerudová má problém. Lidé chtějí za prezidenta starého a hnusného ...

Never more imbecilům na koncertech, které živá hudba nezajímá

„Za jeden prst v zadku ho přece nepošlete sedět." Advokátka Lucie Hrdá o šokujícím...

Prezident X | Odcházení Miloše Zemana | Kalousek & Stoniš | Hodina dějepichu | Byznys X | Seroš X | Audiopovídky Reflexu

Reflex.cz › Byznys X › Kyberútoky jsou chytřejší, pracují i s momentem překvapení. Jak se bránit radí šéf bezpečnosti z České spořitelny

ZAUJALO NÁS

Kyberútoky jsou chytřejší, pracují i s momentem překvapení. Jak se bránit radí šéf bezpečnosti z České spořitelny

Jitka Menclová 24. října 2022 • 11:30

Podvodné reklamy, které nabízí investovat do veřejně známých firem nebo kryptoměn, SMS zprávy zasílané jménem Ministerstva práce a sociálních věci, nebo telefonáty falešných zaměstnanců banky kvůli napadení vašeho účtu. To jsou jen vybrané způsoby podvodníků, které směřují k jedinému – obrat lidi o penize. Jaké praktiky podvodnici používají a jak proti nim bojuje Česká spořitelna, jsme se zeptali šéfa bezpečnosti Josefa Recha.

Reklamy

Fotovoltaika na klíč od ČEZ

Reklama · ČEZ Prodej, a.s.

Sukně k bundě Ice UHIP, dámská, stormy weather blue

Reklama · GLAMI

Jaké věkové skupiny jsou nejvíce ohroženy čím dál častějšími podvody v on-line prostředí?

Nelze říci, že by byla nejvíce ohrožena nějaká věková skupina. S podvody na Internetu se mohou setkat všichni, od studentů až po seniory. Když se díváme na rozložení poškozených klientů, vidíme, že je tam průřez celým zastoupením.

Jde spíše o ženy nebo muže? A plyne z výzkumů i proč?

Z našich dat vidíme, že o něco náchylnější uvěřit podvodům jsou ženy. Z celkového počtu kybernetických útoků je podíl mužu a žen v poměru 40 ku 60%. Pokud bychom se dívali na to, v jaké životní fázi se zrovna oběti útoku nachází, jedná se zejména o klienty středního věku, kteří nemají děti. V naprosté většině jsou útoky podvodníků cílené na občany ČR (86 %), evidujeme ale větší míru phishingových útoků na klienty ukrajinské národnosti (tvoří téměř 10 %). Celkově 6 z 10 klientů mají středoškolské vzdělání zakončené maturitou.

Přečti si nové číslo Reflexu

SMÍCH NABÍJÍ

Tištěné předplatné Reflexu

Tištěné speciály Reflexu

Elektronický archiv Reflexu

Kurzovní lístek ▶ EUROplatby zdarma ▶

EUR	24	24,12
USD	22,56	22,74

Z hlediska geografického, dá se říct, odkud jsou lidé, kteří jsou vůči podvodům méně odolní?

Z geografického pohledu jsou zastoupeny všechny regiony stejně. Naprostá většina klientů využívá digitální bankovnictví George, to platí i pro starší věkovou kategorii.

Jak je to s mladší generací? Jsou i oni náchylní na podvody tohoto typu?

Pokud jde o samotnou formu podvodu, vidíme, že mladší generace je více náchylná podlehnout různým druhům phishingu, kdy se útočník snaží získat citlivé údaje k platební kartě nebo přihlašovací údaje k internetovému bankovnictví. K prvnímu kontaktu obvykle dochází na sociálních sítích.

Mezi pojmy spojenými s podvody se objevují názvy phishing a vishing – o co jde?

Phishing je podvodná technika v on-line prostředí s cílem získat a následně zneužít bezpečnostní údaje k internetovému bankovnictví nebo k platební kartě. Cílem podvodu je předstírat, že jde o komunikaci kurýrní nebo doručovací služby, bank, on-line platebních portálů či úřadů státní správy. Nejčastěji phishing probíhá prostřednictvím e-mailů, SMS zpráv nebo sociálních sítí. Pachatel v podvodné zprávě informuje například o potřebě zadání údajů platební karty, aby se zmiňovaná transakce dokončila, blokaci nebo zneužití internetového bankovnictví, o podezřelých transakcích, a podobně. Snaží se na klienta vyvíjet tlak, aby klikl na daný odkaz, ze kterého se dostane například na falešnou přihlašovací stránku do internetového bankovnictví.

Vishing je v principu podobný útok jako phishing, ale probíhá po telefonu (z anglického voice-phishing). Je to poměrně nový typ podvodu, jejichž počet se v posledním roce více než zdvojnásobil. Nejčastější scénář probíhá tak, že pachatel volá klientovi, přičemž se vydává buď za zaměstnance banky, zaměstnance Česká národní banky nebo příslušníka Policie a snaží se klienta pod nějakou záminkou přimět, aby svou hotovost vybral a následně ji vložil na jiný “bezpečný” účet nebo do kryptoměnového bankomatu. Evidujeme i případy falešných nákupů akcií. Klient je v těchto případech směrován na připravenou webovou stránku, kde jsou připravené rostoucí akciové grafy, ale s investicí klienta nemají nic společného, k žádnému nákupu akcií nedojde.

Jaké jsou nejčastější příčiny, proč se inteligentní člověk nechá „napálit“ a přijde o své peníze?

Jednotlivé útoky jsou stále sofistikovanější, pracují s momentem překvapení nebo apelují na autoritu. Útočníci se představují jako pracovníci bezpečnostního oddělení, oddělení řešení podvodů nebo policie. Volaný pak má pocit vyšší potřeby spolupráce, než kdyby přijal hovor z call centra. Jedné klientce, která si telefonát shodou okolností i nahrála, volali po půlnoci. Byla tak zaskočená, že jim údaje z platební karty málem nadiktovala. Pokud reagujete na zaslaný link z SMSky nebo e-mailu, je nutné dobře zkontrolovat, kam své údaje vyplňujete. Přihlašovací stránky do internetového bankovnictví lze napodobit a stejně tak různé internetové evidenční formuláře. Klíčové je vždy na přihlašovací stránku do svého internetového bankovnictví přistupovat výhradně přes oficiální webovou adresu banky, u nás je to www.csas.cz nebo george.csas.cz.

Jak může moderní banka pomocí svým klientům v boji proti podvodům?

Možnosti banky jsou zejména v oblasti edukace klientů. Nejslabším článkem obrany proti phishingu je bohužel lidská důvěřivost. Dlouhodobě klientům v přímé komunikaci vysvětlujeme, s jakými hrozbami se mohou setkat, zároveň se pravidelně zapojujeme do komunikačních kampaní s cílem co nejvíce klienty o kyberhrozbách informovat. Nedávno jsme například spustili velkou kampaň ve spolupráci s ČBA, ve které si mohou lidé i otestovat své znalosti v oblasti kyberbezpečnosti (www.kybertest.cz), Klíčové doporučení, jak se bránit proti phishingu zní „používat selský rozum, být obezřetný, kde vyplňuji své bezpečností údaje a vždy důkladně číst text, který je uveden v SMS nebo aplikaci”. Například pro přijetí peněz není potřeba kamkoliv zadávat bezpečnostní údaje nebo detaily platební karty, stačí protistraně sdělit číslo účtu.

V odpovědích jak se vyzbrojit na bezpečnost na síti (týká se všech bank a jejich klientů) se objevuje umět tzv. desatero. O co jde?

Bezpečnosti a ochraně dat se věnujeme velmi podrobně na webové stránce www.csas.cz/bezpecnost, kde je vytvořen pěkný rozcestník. Snažíme se zde jednak popisovat veškeré praktiky útočníků a přinášet rady, jak se ubránit podvodníkům. Připravili jsme rovněž řadu vzdělávacích videí a ukázek, jak jednotlivé útoky v praxi probíhají. Již před několika lety vznikla myšlenka sepsat tzv. Bezpečnostní desatero, což je takové minimum informací, které by si měl každý uživatel internetu přečíst.

Jakými moderními prostředky bojuje proti podvodům Česká spořitelna?

Klientské bezpečnosti se věnuje u nás v bance hned několik týmů. Máme celou řadu podpůrných nástrojů, díky kterým dokážeme klientům pomoci. Jedním z vysoce účinných nástrojů je využívání naší aplikace pro potvrzování plateb George klíč. Se zavedením dvoufaktorového potvrzování plateb jsme rovněž přišli s tzv. behaviorální analýzou přímo v digitálním bankovnictví George. Dokážeme tak snižovat počet podvodných kartových transakcí v online prostředí. Zajímavou novinkou je George klíči funkce, díky které si nyní klienti jednoduše ověří, zda jim volá bankéř ze Spořitelny. Věříme, že tak významně snížíme počet podvodných telefonátů, kdy se útočníci vydávají za naše zaměstnance. Obecně ale platí, že i když neustále naše systémy vylepšujeme a hledáme cesty, jak známým podvodům zabránit a klienta včas varovat, pořád platí, že ať budeme mít sebelepší technologie, které zaručí bezpečnost klientů, nejslabším článkem zůstává lidský faktor.

Nabízíte klientům ještě nějaké další služby, které jim mohou pomoci chránit je před kyberhrozbami?

Za zmínku stojí například využívání virtuálních platebních karet při nákupech na internetu. Klientům umožňujeme přímo v mobilním bankovnictví si vytvořit jednorázovou platební kartu, která se po zaplacení zruší a nelze ji tak znovu použít. Klientům přináší jistotu zejména při placení na neprověřených internetových obchodech nebo tam, kde obchodníci nevyžadují dvoufaktorovou metodu potvrzování plateb. Vrátím-li se ještě k aplikaci George klíč, nedávno jsme do něj přidali nový bezpečnostní prvek, který zase o něco více klienty chrání před phishingem. Instalaci této aplikace na dalším zařízení umožňujeme pouze za určitých podmínek. Klient musí mít bluetooth zapnutý na obou mobilních zařízeních, která od sebe nesmí být vzdálena víc než pár metrů.

97.Podvodníci se vydávají za bankéře, úředníky i policisty. Útočí na účty

Online ● ceskobudejovicky.denik.cz (Regionální zprávy) ● 24. 10. 2022, 12:02

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)** ● Autor: **Edwin Otta** ● Rubrika: **Zprávy**

Dosah: 26 183 ● GRP: 0.29 ● OTS: 0.00 ● AVE: 69384.78 Kč ● Interakcí: 4

Odkaz: https://ceskobudejovicky.denik.cz/zlociny-a-soudy/podvodnici-se-vydavaji-za-bankere-uredniky-i-policisty-utoci-na-ucty-20221024.html

24.10.2022

Edwin Otta
Zloději už neběhají po ulicích, kradou pohodlně přes internet. Podvodníci už využívají k obelhání obětí i nejnovější státní příspěvky. Policisté v rámci prevence nabízejí test, který ukáže, jak jste schopni odolat podvodu.
Kliknutím zvětšíte
Podvodníci se vydávají za bankéře, úředníky i policisty. Útočí na účty. Ilustrační foto. | Foto: Archiv
Stačí několik desítek vteřin, maximálně minut a celoživotní úspory nebo všechny peníze z účtů jsou pryč. Zloději vycítili příležitost a podle jihočeského policejního mluvčího Jiřího Matznera vynalézavě využívají možnosti, které poskytuje internet. A oběti často s neuvěřitelnou lehkomyslností s pachateli spolupracují.
K nejnovějším trikům patří SMS či podobná zpráva, že dotyčnému byla schválena žádost o některý z nových státních příspěvků. Následně se ale budoucí oběť dozví, že musí na zadanou webovou stránku poslat své přihlašovací údaje. Česká ministerstva a další úřady už několik desítek takových podvodných stránek zablokovaly, ale přesto jsou v určitém procentu případů zloději úspěšní. Přitom třeba číslo účtu už se zadává při podání žádosti!
Podvody a krádeže, které se dříve děly tváří v tvář se nyní přesouvají na internet. Falešní prodejci, kteří následně vykrádali seniorům kredence, nebo slibovali dodání zboží, které se nikdy neobjevilo, už se teď ani nenamáhají obcházet domácnosti. Využívají telefon a internet a pohodlně "od stolu" kradou i milionové částky.
Můžete se otestovat
Jiří Matzner připomíná, že na policejním webu je přístupný projekt několika institucí - mimo jiné České bankovní asociace nebo Policie ČR. Projekt se nazývá Nepindej a na adrese **kybertest**.cz se tam může každý nejen podívat, kde hrozí nebezpečí, ale také si vyzkoušet, jak podvodníkům odolat. V adresách, které se tváří dokonale, je totiž zavádějící třeba jen jedna tečka nebo podtržítko… Lidé by si podle Jiřího Matznera měli dát pozor vždy, když je někdo žádá o přihlašovací údaje k jejich kontu, související hesla nebo hesla k počítačům či mobilům. "Lidé tomu neuvěřitelně nahrávají," upozorňuje k novému typu zločinů Jiří Matzner.
Navíc je dobré sledovat co se děje "v okolí". "Podvodné maily často chodí ve vlnách, celou republikou projdou v několik týdnech, pak je pár měsíců klid a objeví se nová finta. Oběti často uvěří i velmi neobvyklé nabídce a sami posílají peníze…
Podvodníci lákají například na dědictví. Českobudějovičtí policisté řeší případ, kdy se na Jihočecha obrátil údajný právní zástupce jménem A. Ferrari a nabídl mu dědictví po příbuzném ve výši 19 milionů dolarů. To ale mělo ležet ve španělské bance. Za různé služby a poplatky vydal Jihočech 57 000 korun. Naštěstí už na další výzvu k platbě nereagoval. Ale odeslané finance jsou zřejmě navždy pryč.
Úspěšnost polici je při stíhání těchto deliktů sporadická. Během několika dnů stihnou finance proputovat po různých účtech doslova přes celou zeměkouli, aby je následně bylo možné vybrat kdekoli v cizině nebo i v sousedství okradeného, aniž by prakticky peníze kdo mohl efektivně vysledovat a vrátit.
Naverbovaní rodilí mluvčí
Když se nedávno podařilo Interpolu dopadnout celý gang zlodějů operující na internetu, je to spíše výjimka než pravidlo.
A jestliže v minulosti se mnohý útok vedený z ciziny dal rozpoznat díky špatné češtině, odborníci varují, že zloději si už jazyk zdokonalili k nerozeznání. Dokonce mají mezinárodní skupiny k dispozici rodilé mluvčí. To jsou případy, kdy jsou třeba lidé osloveni, že byl veden útok na jejich peníze v bance. Pokud si chce někdo obezřetnější zjistit více, ozve se mu vzápětí falešný policejní důstojník, který potvrdí, že kvůli ochraně je nutné peníze převést na konto, které doporučili podvodníci vydávající se za bankéře…
Z jiného ranku je nabídka investic, kdy se oběti falešní odborníci vyptávají na znalosti z oboru, aby ukázali, že "příležitost" není pro každého… Zhodnotí pak uloženou částku v řádu týdnů o desítky

procent, na falešných stránkách oběť sleduje, jak jí tuční konto, ale když pošle třeba i několik milionů (!) zmizí najednou všechna dobře připravená kamufláž z internetu a pachatelé samozřejmě beze stopy také.
V některých případech chtějí lidé prodat zboží přes internetové bazary. Aby mohli inkasovat, mají zadat své přihlašovací údaje. Jako v minulých dnech ženy ze Strakonicka a Písecka. Neuvědomí si ani, že jim z účtu peníze naopak mizí ve stejné částce, v jaké jim měly přijít, když si omyl uvědomí je pozdě. A ještě mohou mluvit o štěstí, že si zloději díky získaným kódům nevzali jménem obětí úvěr, často na velkou sumu peněz... To, že nepřijde zboží zaplacené předem přes internet, také ještě podvodníci nevypustili z rejstříku!
Staré triky stále žijí
Obyčejné vydírání, kdy pachatelé hrozí, že prozradí policii, že dotyčný sledoval zakázané pornostránky, už dnes patří skoro historii. Stále se ovšem praktikuje! Stejně jako zavirování počítače a nabídka na uvedení věcí do pořádku při složení požadované částky. Podle odborníků je pak padesát na padesát, jestli pachatelé dodrží slovo a po zaplacení výpalného zařízení odvirují.
Už sice existují i "bílé" hackerské skupiny, které proti blokovacím a viry nesoucím programům dávají veřejně k dispozici programy na pomoc postiženým, ale spoléhat na ně by bylo ošidné.
Jak se tedy bránit? Lze jen zopakovat, že nikomu by se neměly poskytovat přihlašovací údaje internetového bankovnictví. Na internetu nakupovat jen u ověřených prodejců, ověřovat si telefony nebo adresy, uchovávat e-mailovou či SMS komunikaci a nevěřit podezřele výhodným nabídkám.

98. Podvodníci se vydávají za bankéře, úředníky i policisty

Tisk ● Táborský deník; str. 2 (Regionální zprávy) ● 25. 10. 2022

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)**

Dosah: 19 289 ● GRP: 0.21 ● OTS: 0.00 ● AVE: 76665.51 Kč

Odkaz: náhled

TÁBORSKO | Jižní Čechy

ČTENÁŘ REPORTÉR deník

Lucie Čmuchová

Filmový festival podpořil lidi s autismem

V divadle Oskara Nedbala v Táboře se konal Filmový festival o autismu. Nechyběl ani francouzský film Výjimeční o práci s autisty. Festival se konal k 15. výročí organizace APLA JČ (pro aktivní podporu lidí s autismem).

V doprovodném programu proběhla i kratší projekce o Homesharingu (přirozený způsob podpory rodin dětí s intelektuálním či kombinovaným znevýhodněním) a nechyběla debata s Danem Samcem na téma odlehčovací péče o lidi s autismem z vlastní zkušenosti. Akce se vydařila a návštěvníci přišli v hojném počtu.

Eva Gardošová

Dračí slet v mateřské škole Hastrmánek

Podzimní slunečné čtvrteční odpoledne na louce pod Kauflandem patřilo opět jednou za rok papírovým drakům dětí z MŠ Hastrmánek v Táboře. Radostné vítání dračích kamarádů nebralo konce. Vždyť v jednu chvíli jsme jich napočítali i sto. Oblohu zdobily duhové čtverce, motýlci, orlí i pohádkové postavičky a děti zase dračí náramky, vyrobené učitelkami. Nádherná podívaná, šťastné děti pobíhající po louce i spokojení rodiče nám dovolili zapomenout alespoň pro tuto chvíli na starosti a povinnosti všedního dne.

(Foto: Marie Kalafutová)

Poslední rozloučení

Úterý 25. října, smuteční síň Tábor
9.30 h Miroslav Pechánek (1962), Nová Ves u Chýnova
11 h Bc. Josef Pilař (1978), Tábor
13.15 h Věra Urbanová (1946), Choustník
Středa 26. října, smuteční síň Tábor
11 h Hana Hejná (1944), Tábor
12.30 h Jaroslava Hašplová (1943), Čenkov

I vaše narozené miminko může být v Deníku

Narodilo se vám miminko a chcete si tuto chvíli pamatovat? Své děťátko můžete najít na stránce našich novin ještě dříve, než vyslovíš své první slovo. Stačí poslat jeho fotku spolu s dalšími údaji (jménem, váhou, jmény rodičů a případně sourozenců, bydlištěm, datem a místem narození) na e-mailovou adresu **mimina.jc@denik.cz** a své miminko najdete v sobotním Deníku a na webových stránkách.

Podvodníci se vydávají za bankéře, úředníky i policisty

Na policejním webu je přístupný projekt několika institucí – mimo jiné České bankovní asociace nebo Policie ČR. Nazývá se Nepindej a na adrese kybertest.cz se může každý nejen podívat, kde hrozí nebezpečí, ale také si vyzkoušet, jak podvodníkům odolat. V adresách, které se tváří dokonale, je totiž zavádějící třeba jen jedna tečka nebo podtržítko…

BANKY I POLICIE varují před podvodníky. Foto: archiv Deníku

Jižní Čechy – Lidé by si podle Jiřího Matznera měli dát pozor vždy, když je někdo žádá o přihlašovací údaje k jejich kontu, související hesla nebo hesla k počítačům či mobilům. „Lidé tomu neuvěřitelně nahrávají," upozorňuje policejní mluvčí.

Navíc je dobré sledovat co se děje „v okolí". Podvodné e-maily často chodí ve vlnách, republikou projdou v několik týdnech, pak je pár měsíců klid a objeví se nová finta. Oběti často uvěří i velmi neobvyklé nabídce a sami posílají peníze…

Podvodníci lákají například na dědictví. Českobudějovičtí policisté řeší případ, kdy se na Jihočecha obrátil údajný právní zástupce a nabídl mu dědictví po příbuzném ve výši 19 milionů dolarů. To ale mělo ležet ve španělské bance. Za poplatky vydal Jihočech 57 000 korun. Naštěstí už na další výzvu k platbě nereagoval. Ale odeslané peníze jsou zřejmě navždy pryč. Úspěšnost policie je při stíhání těchto deliktů sporadická.

RODILÍ MLUVČÍ

Jestliže se v minulosti dal mnohý útok vedený z ciziny rozpoznat díky špatné češtině, odborníci varují, že zloději si už jazyk zdokonalili k nerozeznání. Dokonce mají mezinárodní skupiny k dispozici rodilé mluvčí. To jsou případy, kdy jsou třeba lidé osloveni, že byl veden útok na jejich peníze v bance. Pokud si chce někdo obezřetnější zjistit více, ozve se mu vzápětí falešný policejní důstojník, který potvrdí, že kvůli ochraně je nutné peníze převést na konto, které doporučili podvodníci vydávající se za bankéře. Z jiného ranku je nabídka investic, kdy se falešní odborníci vypřádají oběti na znalosti z oboru, aby ukázali, že „příležitost" není pro každého.

Zhodnotí uloženou částku v řádu týdnů o desítky procent, na falešných stránkách oběť sleduje, jak jí tuční konto, ale když pošle třeba i několik milionů, zmizí najednou dobře připravená kamufláž z internetu.

V některých případech chtějí lidé prodat zboží přes internetové bazary. Aby mohli inkasovat peníze, mají zadat své přihlašovací údaje. Jako v minulých dnech ženy ze Strakonicka a Písecka. Neuvědomí si ani, že jim z účtu peníze naopak mizí ve stejné částce, v jaké jim měly přijít.

STARÉ TRIKY JEŠTĚ ŽIJÍ

Obyčejné vydírání, kdy pachatelé hrozí, že prozradí, že dotyčný sledoval pornostránky, už dnes patří skoro historii. I to se se však stále praktikuje! Stejně jako zavirování počítače a nabídka na uvedení věcí do pořádku při složení požadované částky.

Jak se tedy bránit? Nikomu by se neměly poskytovat přihlašovací údaje do internetového bankovnictví. Na internetu nakupovat u ověřených prodejců a nevěřit výhodným nabídkám. **(win)**

Cesta do kostela měla tečku v podobě ocenění

Strakonice – Letos v červnu obdržela ředitelka Muzea středního Pootaví Strakonice Ivana Říhová od Suverénního řádu maltézských rytířů cenné vyznamenání. Je to Maltézský záslužný řád (Ordine pro Merito Melitensi). Uděluje se osobám, které se výjimečně zasloužily o maltézský řád. „Když si na ty chvíle vzpomenu, citím velké dojetí," říká Ivana Říhová.

Když jsme spolu mluvili krátce po udělení řádu, svěřila jste se, že jste nic takového neočekávala.

To je pravda. Jezdíme každoročně na svátek sv. Jana Křtitele 24. června na slavnostní bohoslužbu do kostela Panny Marie pod řetězem na Malé Straně. Před začátkem mne pan ředitel úřadu sv. Jana Jeruzalémského řekl, že pan velvyslanec by mi chtěl osobně poděkovat. Řekla jsem si, proč ne. Dostanu kytičku a poděkujeme si navzájem.

Jenže to bylo trochu jinak.

Úplně jinak. Přišel pan velvyslanec a nesl červenou krabičku a kytici. Nebudu lhát, byla jsem překvapená a dojatá. Jde totiž o vysoké ocenění, jehož se rozhodně nedostane každému.

Můžete vyznamenání představit?

Je to oficiální řád maltézského řádu, který mi na popud českého velkopřevorství udělil velmistr v Římě. Má tři stupně – medaile, kříž a ozdobný obojek. Já jsem získala kříž.

IVANA ŘÍHOVÁ s významným oceněním. Foto: Deník/Petr Škotko

K vyznamenání patří listina.

Přesně tak. V ní se víceméně píše, že jsem si řád zasloužila. Ale pravda je taková, že toto ocenění patří celému muzeu.

Listina je psaná latinsky a dole vlevo je číslo. Jaký má význam?

Je zde 3011, což znamená, že jsme od roku 1920, kdy se ocenění předává, jeho 3011. držitelem.

Můžete připomenout důvod ocenění?

V muzeu ve Strakonicích máme expozici věnovanou historii a současnosti řádu maltézských rytířů. V České republice ani v Evropě druhá taková není. **(pš)**

PEKELNÁ JÍZDA NADCHLA FANOUŠKY METALU

JIŽ POOSMNÁCTÉ mohli fanoušci tvrdší hudby navštívit tradiční mladovožickou Pekelnou jízdu. Hudebním nadšencům pak organizátoři v klubu High Ground naservírovali koncert v podání kapel Törr, Nine Six Nine a Psychohlina. Koncerty, na nichž vždy vystoupí několik punkových či metalových kapel, pořádá skupinka nadšenců již od roku 2009. „Příprava jednoho koncertu nám trvá přibližně tři měsíce a vše chystáme zhruba v deseti lidech. Dříve se hrálo dvakrát do roka, teď už jenom jednou. Jeden rok jsme dokonce úplně vynechali. Většina z nás totiž už máme děti a na přípravu tak není tolik času," vysvětlila jedna z organizátorek Eva Pudilová. Pekelnou jízdu si v pátek večer vychutnalo kolem 180 návštěvníků.

Foto: Deník/Jiří Dintar

DENÍK V JIHOČESKÝCH MUTACÍCH: Českobudějovický deník, Českokrumlovský deník, Prachatický deník, Strakonický deník, Písecký deník, Táborský deník, Jindřichohradecký deník. Vychází pondělí – sobota. Vydává VLTAVA LABE MEDIA a.s., U Trezorky 921/2, Jinonice, 158 00 Praha 5, IČ 01440578. Předseda představenstva a generální ředitel: Vít Nantl. CENTRÁLNÍ REDAKCE: U Trezorky 921/2, Jinonice, 158 00 Praha 5. Od 1. 1. 2022 je platný ceník inzerce č. 22.
REGION JIŽNÍ ČECHY: Náměstí Přemysla Otakara II. 8/5, 370 01 České Budějovice. **Manažer inzerce:** Pavla Pudivítrová, e-mail: pavla.pudivitrova@vltmedia.cz. Šéfredaktor redakcí v jižních Čechách: Kamil Kacerovský, šéfeditor redakcí v jižních Čechách: Martin Trister.
TÁBORSKÝ DENÍK: Náměstí Přemysla Otakara II. 8/5, 370 01 České Budějovice, redakce.taborsky@denik.cz. **Šéfredaktor Táborského deníku:** Jiří Dintar, e-mail: jiri.dintar@denik.cz, mobil: 602 667 657. **Příspěvky čtenářů:** Kamila Šmídová, mobil: 602 667 636, e-mail: kamila.smidova@denik.cz. **Sport:** Pavel Šacha, e-mail: pavel.sacha@denik.cz, mobil: 606 129 972. **Manažer distribuce:** Roman Dvořák, e-mail: roman.dvorak@denik.cz. **Inzerce:** Marketa Jenčíková, e-mail: marketa.jenclikova@denik.cz, tel. 736 166 183. **Servis pro čtenáře, řádková inzerce:** inzerce.radkova.JC@vltmedia.cz. Texty označené PR, PI jsou placená inzerce. **Tiskne:** VLTAVA LABE MEDIA a.s., tiskárna Novotisk Praha. **Ročník:** XVIII, ISSN 1210-7352, MK ČR E6566. Prodaný náklad ověřuje ABC ČR, Pobřežní 370/4, 186 00 Praha 8. Nevyžádané rukopisy a fotografie se nevracejí. Předplatné doručuje: Mediaservis, s.r.o. Deník najdete také v aplikacích pro iPhone a OS Android. **Centrum zákaznické péče: 272 015 015, 272 015 020.** E-mail: denik@mojepredplatne.cz, více: www.mojepredplatne.cz. V případě reklamace doručení nás, prosím, kontaktujte na el. adrese reklamace@denik.cz.

99. Podvodníci se vydávají za bankéře, úředníky i policisty

Tisk • Českobudějovický deník; str. 2 (Regionální zprávy) • 25. 10. 2022

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)**

Dosah: 9 946 • GRP: 0.11 • OTS: 0.00 • AVE: 40138.59 Kč

Odkaz: náhled

2 Deník www.denik.cz 25. října 2022

ČESKOBUDĚJOVICKO | Jižní Čechy

Podvodníci se vydávají za bankéře, úředníky i policisty

Zloději už neběhají po ulicích, kradou pohodlně přes internet. Podvodníci využívají k obelhání obětí i nejnovější státní příspěvky. Policisté v rámci prevence nabízejí test, který ukáže, jak jste schopni odolat podvodu.

EDWIN OTTA

Jižní Čechy – Stačí několik desítek vteřin, maximálně minut a celoživotní úspory nebo všechny peníze z účtu jsou pryč. Zloději vycítili příležitost a podle jihočeského policejního mluvčího Jiřího Matznera vynalézavě využívají možnosti, které poskytuje internet. A oběti často s neuvěřitelnou lehkomyslností s pachateli „spolupracují".

K nejnovějším trikům patří SMS či podobná zpráva, že dotyčnému byla schválena žádost o některý z nových státních příspěvků. Následně se ale budoucí oběť dozví, že musí na zadanou webovou stránku poslat své přihlašovací údaje. Česká ministerstva a další úřady už několik desítek takových podvodných stránek zablokovaly, ale přesto jsou v určitém procentu případů zloději úspěšní. Přitom třeba číslo účtu už se zadává při podání žádosti!

KRADOU „OD STOLU"

Podvody a krádeže, které se dříve děly tváří v tvář se nyní přesouvají na internet. Falešní prodejci, kteří kradli seniorům úspory z kredence nebo slibovali dodání zboží, které se však nikdy neobjevilo, už se teď ani nenamáhají obcházet domácnosti. Využívají jenom telefon a internet a pohodlně takzvaně „od stolu" kradou i milionové částky.

Jiří Matzner připomíná, že na policejním webu je přístupný projekt několika institucí – mimo jiné České bankovní asociace nebo Policie ČR. Projekt se nazývá Nepindej a na adrese kybertest.cz se tam může každý nejen podívat, kde hrozí nebezpečí, ale také si vyzkoušet, jak podvodníkům odolat. V adresách, které se tváří dokonale, je totiž zavádějící třeba jen jedna tečka nebo podtržítko...

Lidé by si podle Jiřího Matznera měli dát pozor vždy, když je někdo žádá o přihlašovací údaje k jejich kontu, související hesla nebo hesla k počítačům či mobilům. „Lidé tomu neuvěřitelně nahrávají," upozorňuje policejní mluvčí.

Navíc je dobré sledovat co se děje „v okolí". Podvodné e-maily často chodí ve vlnách, republikou projdou v několik týdnech, pak je pár měsíců klid a objeví se nová finta. Oběti často uvěří i velmi neobvyklé nabídce a sami posílají peníze...

Podvodníci lákají například na dědictví. Českobudějovičtí policisté řeší případ, kdy se na Jihočecha obrátil údajný právní zástupce a nabídl mu dědictví po příbuzném ve výši 19 milionů dolarů. To ale mělo ležet ve španělské bance. Za poplatky vydal Jihočech 57 000 korun. Naštěstí už na další výzvu k platbě nereagoval. Ale odeslané peníze jsou zřejmě navždy pryč. Úspěšnost policie je při stíhání těchto deliktů sporadická. Během několika dnů stihnou finance proputovat po různých účtech doslova přes celou zeměkouli, aby je následně bylo možné vybrat kdekoli v cizině nebo i v sousedství okradeného, aniž by prakticky peníze kdo mohl efektivně vysledovat a vrátit.

Když se nedávno podařilo Interpolu dopadnout celý gang operující na internetu, byla to spíše výjimka než pravidlo.

RODILÍ MLUVČÍ

Jestliže se v minulosti dal mnohý útok vedený z ciziny rozpoznat díky špatné češtině, odborníci varují, že zloději si už jazyk zdokonalili k nerozeznání. Dokonce mají mezinárodní skupiny k dispozici rodilé mluvčí. To jsou případy, kdy jsou třeba lidé osloveni, že byl veden útok na jejich peníze v bance. Pokud si chce někdo obezřetnější zjistit více, ozve se mu vzápětí falešný policejní důstojník, který potvrdí, že kvůli ochraně je nutné peníze převést na konto, které doporučili podvodníci vydávající se za bankéře. Z jiného ranku je nabídka investic, kdy se falešní odborníci vyptávají obětí na znalosti z oboru, aby ukázali, že „příležitost" není pro každého. Zhodnotí uloženou částku v řádu týdnů o desítky procent, na falešných stránkách oběť sleduje, jak jí tuční konto, ale když pošle třeba i několik milionů, zmizí najednou dobře připravená kamufláž z internetu.

V některých případech chtějí lidé prodat zboží přes internetové bazary. Aby mohli inkasovat peníze, mají zadat své přihlašovací údaje. Jako v minulých dnech ženy ze Strakonicka a Písecka. Neuvědomí si ani, že jim z účtu peníze naopak mizí ve stejné částce, v jaké jim měly přijít. A ještě mohou mluvit o štěstí, že si zloději díky získaným kódům nevzali jménem obětí úvěr, často na velkou sumu peněz... To, že nepřijde zboží zaplacené předem přes internet, také stále podvodníci nevypustili z rejstříku!

STARÉ TRIKY JEŠTĚ ŽIJÍ

Obyčejné vydírání, kdy pachatelé hrozí, že prozradí, že dotyčný sledoval pornostránky, už dnes patří skoro historii. I to se se však stále praktikuje! Stejně jako zavirování počítače a nabídka na uvedení věci do pořádku při složení požadované částky.

Jak se tedy bránit? Lze jen zopakovat, že nikomu by se neměly poskytovat přihlašovací údaje internetového bankovnictví. Na internetu nakupovat jen u prověřených prodejců, ověřovat si telefony nebo adresy, uchovávat e-mailovou či SMS komunikaci a nevěřit podezřele výhodným nabídkám.

BANKY I POLICIE varují před podvodníky. Foto: archiv Deníku

100. Index Kyberbezpečnosti 2022

Online ● cbaonline.cz ((nezařazené)) ● 25. 10. 2022, 12:10

Dosah: 950 ● GRP: 0.01 ● OTS: 0.00 ● AVE: 5241.02 Kč

Odkaz: https://cbaonline.cz/index-kyberbezpecnosti-2022

Index Kyberbezpečnosti 2022 se drží na vysoké úrovni. Kybertestem prošly desítky tisíc lidí.

Češi jsou v online prostoru opatrní. Index Kyberbezpečnosti dosáhl 67 bodů a drží se tak blízko výsledku z loňského roku. Finanční operace lidé považují za citlivé a k internetovému či mobilnímu bankovnictví by nikdy neposkytla přístup většina z nich. Banky jsou pro Čechy nejdůvěryhodnější instituce, pokud jde o ochranu před únikem dat. Vyplývá to z průzkumu České bankovní asociace a výzkumné agentury Ipsos. Výsledkům průzkumu odpovídají i průběžná data Kybertestu, kterým během necelých dvou měsíců prošlo 54 tisíc lidí s průměrným výsledkem 70 %.

Index Kyberbezpečnosti dosáhl 67 bodů, o jeden bod méně než loni.

V loňském roce byly výsledky nejlepší od začátku sledování, index dosáhl 68 bodů. Letos je výsledek jen nepatrně nižší. Výsledky jsou z různých hledisek velmi vyrovnané. Lidé se základním vzděláním získali v průměru 65 bodů, zatímco vysokoškolsky vzdělaní získali průměrně 68 bodů.

„Zdá se, že lidé si uvědomují rizika, která jsou s online prostředím spojená. Naprostá většina by neposkytla přístupové údaje do internetového bankovnictví. Téměř dvě třetiny lidí kontrolují výdaje a úspory na účtu pravidelně,“ říká **Petr Barák**, expert České bankovní asociace na finanční a bankovní bezpečnost.

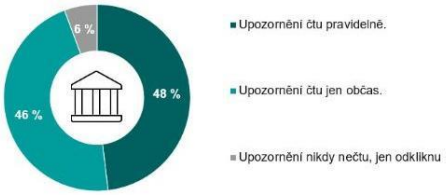
Češi jsou ve sdílení informací opatrní, čtvrtina ale někdy otevře neznámou přílohu

Za žádných okolností by přihlašovací údaje k účtu neposkytlo 86 % Čechů. Víc než polovina by nesdílela ani výši svých úspor, číslo platební karty nebo rodinné fotografie. Další informace jsou lidé ochotni sdělit pouze za určitých okolností. Více než tři čtvrtiny se v takových případech podělí o telefonní číslo a adresu trvalého bydliště. Téměř tři čtvrtiny lidí neotvírají přílohy od neznámých odesílatelů, čtvrtina však alespoň některou otevře. Upozornění banky na možné hrozby čte většina lidí a přibližně polovina to dokonce dělá pravidelně. Osm z deseti Čechů se do svého internetového bankovnictví připojuje přes vlastní zařízení, které je zcela pod jejich kontrolou.

„Česká populace je poměrně obezřetná v případě sdělování citlivých osobních údajů jako je číslo platební karty či přihlašovací údaje k bankovnímu účtu. Na druhou stranu však nemalá část lidí, přibližně čtvrtina, alespoň někdy otevírá přílohy emailů od neznámých uživatelů, což může způsobit vážný problém“ uvádí **Michal Straka** z agentury Ipsos.

Bankám věří lidé v ochraně údajů nejvíc

Banky, pojišťovny či spořitelny jsou považovány za nejbezpečnější, co se týče ochrany před únikem dat. Za důvěryhodné je považuje 59 % Čechů. Oproti tomu státní správu (e-government) vnímá bezpečně pouze necelá třetina. Nejnižší důvěru mají u lidí fintech společnosti, nebankovní poskytovatelé půjček a obchodní řetězce.



Hackerských útoků přibývá, 27 % Čechů se s útokem setkalo letos

Víc než polovina Čechů se stala obětí hackerského útoku, a to bez ohledu na jeho dokončení. Třetina pak zná někoho, kdo byl obětí dokončeného útoku. Nejčastěji jde o podvodné e-maily, které slibují výhru v soutěži, popřípadě velké dědictví od zapomenutého člena rodiny. Víc než polovina má antivirový program v mobilním telefonu, u stolních počítačů je to sedm z deseti lidí. S útokem se nejčastěji setkávají lidé mezi 18 a 34 lety. 27 % Čechů se s útokem setkalo letos. Těmto údajům odpovídají i čísla České bankovní asociace. Počet útoků se za poslední dva roky zvýšil čtyřnásobně a průměrná škoda u dokončeného útoku je na jednoho klienta 162 tisíc korun. Útočníci nejčastěji cílí na získání přihlašovacích údajů, a to ve 40 % případů. Téměř třetina se pak snažila získat číslo platební karty a čtvrtina se zaměřila na osobní údaje, jako je například rodné číslo. Zájem byl také o heslo nebo PIN, a to ve 22 % případů.

Vlastní zkušenost **Dokončený útok v okolí**

Do elektronického bankovnictví se lidé nejčastěji připojují přes Wi-Fi

Lidé se přes Wi-Fi připojují pouze v případech, kdy je dobře zabezpečená. Ve zvyku to má 44 % z nich. Více než čtvrtina lidí se pak připojuje kdekoli, a to pomocí datového tarifu. Na veřejných sítích své finance spravuje pouze 8 % Čechů. Šest z deseti lidí je běžně používají na vyřizování svých e-mailů a jiné korespondence. Téměř polovina (44 %) se pak tímto způsobem přihlašuje na sociální sítě.

„Připojovat se na veřejné, nezaheslované Wi-Fi není nikdy bezpečné. Nicméně lidé to dělají a budou dělat. Po připojení na veřejnou síť musí být lidé velmi ostražití a vstupovat do svého internetového či mobilního bankovnictví by vůbec neměli. Řada lidí si to ale stále neuvědomuje a kvůli tomu na sebe prozradí informace, které by prozrazovat neměli," říká **Milan Habrcetl**, Cyber Security Specialist společnosti Cisco.

Obchodování na on-line bazarech je časté, podvodné telefonáty lidé většinou odhalí

Téměř polovina Čechů někdy nakupovala na on-line bazarech a více než třetina na nich nějaké zboží prodávala. Nejčastější formou platby byl bankovní převod, ve čtyřech případech z deseti pak šlo o osobní předání. Podvodníci se často zaměřují právě na prodávající. Takových případů letos výrazně přibylo.

„Protože jsou prodávající klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům nebo do jejich internetového bankovnictví. Aby co nejdříve docílili prodeje zboží, neopatrně spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně. Opak je bohužel pravdou, většinou o všechno přijdou" objasnil **pplk. Ondřej Kapr** z Policie ČR.

Pouze 3 % lidí by poskytla informace při falešném telefonátu. Víc než polovina z nich by pak situaci ověřila u banky.

Kybertest si vyzkoušely desítky tisíc lidí, úspěšnost je v průměru 70 %

Česká bankovní asociace ve spolupráci s partnery v září spustila celonárodní kampaň #nePINDej! která má za cíl přivést lidi na stránky Kybertest.cz a tímto způsobem je vzdělávat. Za necelé dva měsíce od spuštění Kybertestu kampaň přilákala téměř 54 tisíc lidí, kteří testem prošli v průměru se 70% úspěšností. Kybertest se skládá z deseti nejčastějších podvodů a lidé si tak mohou vyzkoušet, jak odolní jsou proti případným hackerským útokům.

ČBA nedávno spustila i obdobu Kybertestu pro mladší generaci. Kyberhra.cz cílí na žáky druhého stupně základních škol, středních škol a odborných učilišť a víceletých gymnázií. Podvodníci si totiž své cíle vybírají napříč všemi generacemi, bez rozdílu věku či vzdělání.

„V Thein Security si velmi dobře uvědomujeme sílu edukace v našem oboru. Šíření povědomí o bezpečném chování na internetu mezi běžné uživatele je to nejmenší, čím můžeme přispět. A přitom to nejzákladnější. Oceňujeme, že na problematiku upozorňují také silné společnosti, jako je právě Česká bankovní Asociace, jejíž aktivita má celostátní záběr napříč všemi věkovými skupinami. Těší

Asociace, jejíž aktivita má celostátní zásah napříč všemi věkovými skupinami. Těší nás, že jsme mohli být díky naší odbornosti v kybernetické bezpečnosti u tvorby Kybertestu a dosavadní pozitivní ohlasy nás ujišťují, že celá kampaň má skutečně velký smysl," říká Jan Pinta, kyberbezpečnostní expert Thein Security.

Mladiství jsou snadným cílem podvodníků také proto, že se v kyberprostoru pohybují velmi často. Mají chytrá zařízení, ale přesně nevědí, jak se v on-line prostředí bezpečně chovat.

O České bankovní asociaci

Česká bankovní asociace vznikla v roce 1990 a je dobrovolným sdružením právnických osob podnikajících v oblasti peněžnictví. V současné době sdružuje 34 členů. Rolí asociace je především zastupovat a prosazovat společné zájmy členů, prezentovat roli a zájmy bankovnictví vůči veřejnosti, podílet se na standardizaci postupů v bankovnictví a na vytváření odborných zvyklostí, podporovat harmonizaci bankovní legislativy s legislativou Evropské unie a vyvíjet aktivitu v informativní a školící oblasti. ČBA je členem Evropské bankovní federace a EMMI. Více informací na www.cbaonline.cz.

Další dotazy zodpovíme na adrese: radek.salsa@cbaonline.cz

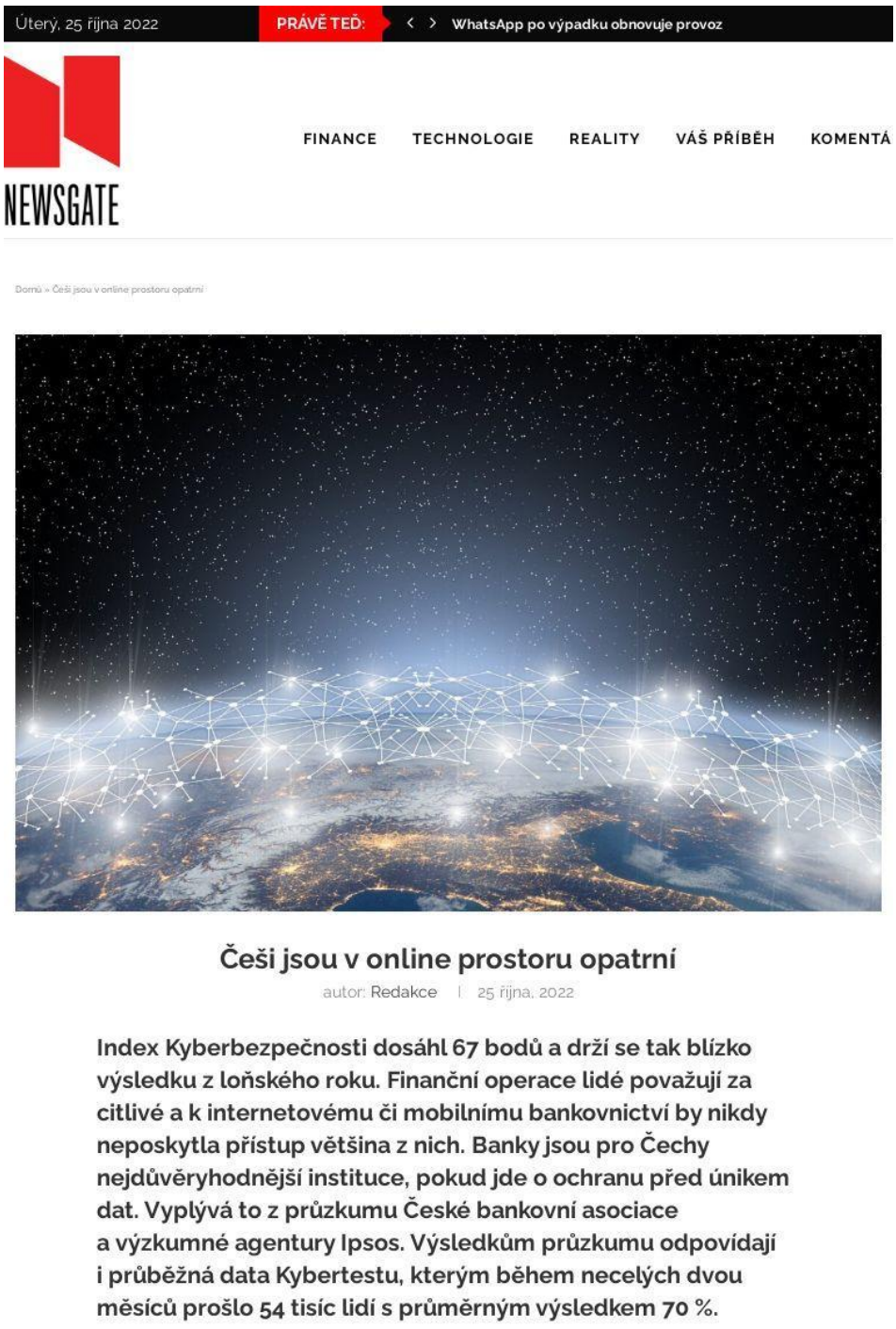
101. Češi jsou v online prostoru opatrní

Online ● newsgate.cz (Zprávy / Politika) ● 25. 10. 2022, 12:23

Vydavatel: **Newsgate s.r.o. (cz-10977350)** ● Rubrika: **Nejčtěnější**

Dosah: 720 ● GRP: 0.01 ● OTS: 0.00 ● AVE: 4511.25 Kč

Odkaz: http://newsgate.cz/nejctenejsi/cesi-jsou-v-online-prostoru-opatrni/



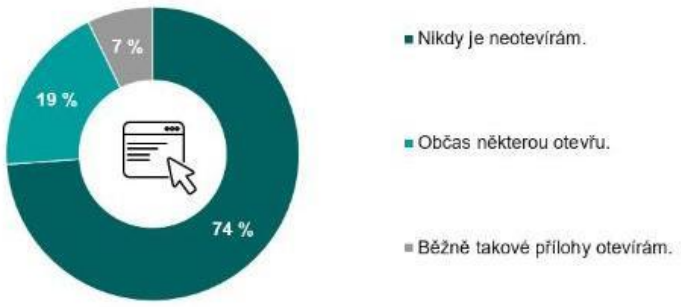
Index Kyberbezpečnosti dosáhl 67 bodů, o jeden bod méně než loni.

V loňském roce byly výsledky nejlepší od začátku sledování, index dosáhl 68 bodů. Letos je výsledek jen nepatrně nižší. Výsledky jsou z různých hledisek velmi vyrovnané. Lidé se základním vzděláním získali v průměru 65 bodů, zatímco vysokoškolsky vzdělaní získali průměrně 68 bodů.

> ***„Zdá se, že lidé si uvědomují rizika, která jsou s online prostředím spojená. Naprostá většina by neposkytla přístupové údaje do internetového bankovnictví. Téměř dvě třetiny lidí kontrolují výdaje a úspory na účtu pravidelně,“*** říká Petr Barák, expert České bankovní asociace na finanční a bankovní bezpečnost.

Češi jsou ve sdílení informací opatrní, čtvrtina ale někdy otevře neznámou přílohu

Za žádných okolností by přihlašovací údaje k účtu neposkytlo 86 % Čechů. Víc než polovina by nesdílela ani výši svých úspor, číslo platební karty nebo rodinné fotografie. Další informace jsou lidé ochotni sdělit pouze za určitých okolností. Více než tři čtvrtiny se v takových případech podělí o telefonní číslo a adresu trvalého bydliště. Téměř tři čtvrtiny lidí neotvírají přílohy od neznámých odesílatelů, čtvrtina však alespoň některou otevře. Upozornění banky na možné hrozby čte většina lidí a přibližně polovina to dokonce dělá pravidelně. Osm z deseti Čechů se do svého internetového bankovnictví připojuje přes vlastní zařízení, které je zcela pod jejich kontrolou.



> ***„Česká populace je poměrně obezřetná v případě sdělování citlivých osobních údajů jako je číslo platební karty či přihlašovací údaje***

> ***k bankovnímu účtu. Na druhou stranu však nemalá část lidí, přibližně čtvrtina, alespoň někdy otevírá přílohy emailů od neznámých uživatelů, což může způsobit vážný problém"*** uvádí Michal Straka z agentury Ipsos.

Bankám věří lidé v ochraně údajů nejvíc

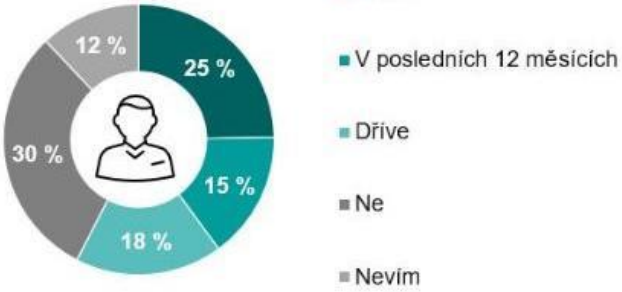
Banky, pojišťovny či spořitelny jsou považovány za nejbezpečnější, co se týče ochrany před únikem dat. Za důvěryhodné je považuje 59 % Čechů. Oproti tomu státní správu (e-government) vnímá bezpečně pouze necelá třetina. Nejnižší důvěru mají u lidí fintech společnosti, nebankovní poskytovatelé půjček a obchodní řetězce.

Hackerských útoků přibývá, 27 % Čechů se s útokem setkalo letos

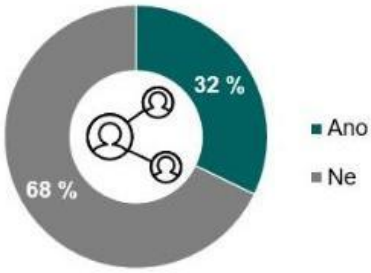
Víc než polovina Čechů se stala obětí hackerského útoku, a to bez ohledu na jeho dokončení. Třetina pak zná někoho, kdo byl obětí dokončeného útoku. Nejčastěji jde o podvodné e-maily, které slibují výhru v soutěži, popřípadě velké dědictví od zapomenutého člena rodiny. Víc než polovina má antivirový program v mobilním telefonu, u stolních počítačů je to sedm z deseti lidí. S útokem se nejčastěji setkávají lidé mezi 18 a 34 lety. 27 % Čechů se s útokem setkalo letos. Těmto údajům odpovídají i čísla České bankovní asociace. Počet útoků se za poslední dva roky zvýšil čtyřnásobně a průměrná škoda u dokončeného útoku je na jednoho klienta 162 tisíc korun. Útočníci nejčastěji cílí na

získání přihlašovacích údajů, a to ve 40 % případů. Téměř třetina se pak snažila získat číslo platební karty a čtvrtina se zaměřila na osobní údaje, jako je například rodné číslo. Zájem byl také o heslo nebo PIN, a to ve 22 % případů.

Vlastní zkušenost



Dokončený útok v okolí



Do elektronického bankovnictví se lidé nejčastěji připojují přes Wi-Fi

Lidé se přes Wi-Fi připojují pouze v případech, kdy je dobře zabezpečená. Ve zvyku to má 44 % z nich. Více než čtvrtina lidí se pak připojuje kdekoli, a to pomocí datového tarifu. Na veřejných sítích své finance spravuje pouze 8 % Čechů. Šest z deseti lidí je běžně používají na vyřizování svých e-mailů a jiné korespondence. Téměř polovina (44 %) se pak tímto způsobem přihlašuje na sociální sítě.

> ***„Připojovat se na veřejné, nezaheslované Wi-Fi není nikdy bezpečné. Nicméně lidé to dělají a budou dělat. Po připojení na veřejnou síť musí být lidé velmi ostražití a vstupovat do svého internetového či mobilního bankovnictví by vůbec neměli. Řada lidí si to ale stále neuvědomuje a kvůli tomu na sebe prozradí informace, které by prozrazovat neměli,“*** říká Milan Habrcetl, Cyber Security Specialist společnosti Cisco.

Obchodování na on-line bazarech je časté, podvodné telefonáty lidé většinou odhalí

Téměř polovina Čechů někdy nakupovala na on-line bazarech a více než třetina na nich nějaké zboží prodávala. Nejčastější formou platby byl bankovní převod, ve čtyřech případech z deseti pak šlo o osobní předání. Podvodníci se často zaměřují právě na prodávající. Takových případů letos výrazně přibylo.

> ***„Protože jsou prodávající klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům nebo do jejich internetového bankovnictví. Aby co nejdříve docílili prodeje zboží, neopatrně spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně. Opak je bohužel pravdou, většinou o všechno přijdou“*** objasnil pplk. Ondřej Kapr z Policie ČR.

Pouze 3 % lidí by poskytla informace při falešném telefonátu. Víc než polovina z nich by pak situaci ověřila u banky.

Kybertest si vyzkoušely desítky tisíc lidí, úspěšnost je v průměru 70 %

Česká bankovní asociace ve spolupráci s partnery v září spustila celonárodní kampaň #nePINDej! která má za cíl přivést lidi na stránky Kybertest.cz a tímto způsobem je vzdělávat. Za necelé dva měsíce od spuštění Kybertestu kampaň přilákala téměř 54 tisíc lidí, kteří testem prošli v průměru se 70% úspěšností. Kybertest se skládá z deseti nejčastějších podvodů a lidé si tak mohou vyzkoušet, jak odolní jsou proti případným hackerským útokům.

ČBA nedávno spustila i obdobu Kybertestu pro mladší generaci. Kyberhra.cz cílí na žáky druhého stupně základních škol, středních škol a odborných učilišť a víceletých gymnázií. Podvodníci si totiž své cíle vybírají napříč všemi generacemi, bez rozdílu věku či vzdělání.

> ***„V Thein Security si velmi dobře uvědomujeme sílu edukace v našem oboru. Šíření povědomí o bezpečném chování na internetu mezi běžné uživatele je to nejmenší, čím můžeme přispět. A přitom to nejzákladnější. Oceňujeme, že na problematiku upozorňují také silné společnosti, jako je právě Česká bankovní Asociace, jejíž aktivita má celostátní zásah napříč všemi věkovými skupinami. Těší nás, že jsme mohli být díky naší odbornosti v kybernetické bezpečnosti u tvorby Kybertestu a dosavadní pozitivní ohlasy nás ujišťují, že celá kampaň má skutečně velký smysl,“*** říká Jan Pinta, kyberbezpečnostní expert Thein Security.

Mladiství jsou snadným cílem podvodníků také proto, že se v kyberprostoru pohybují velmi často. Mají chytrá zařízení, ale přesně nevědí, jak se v on-line prostředí bezpečně chovat.

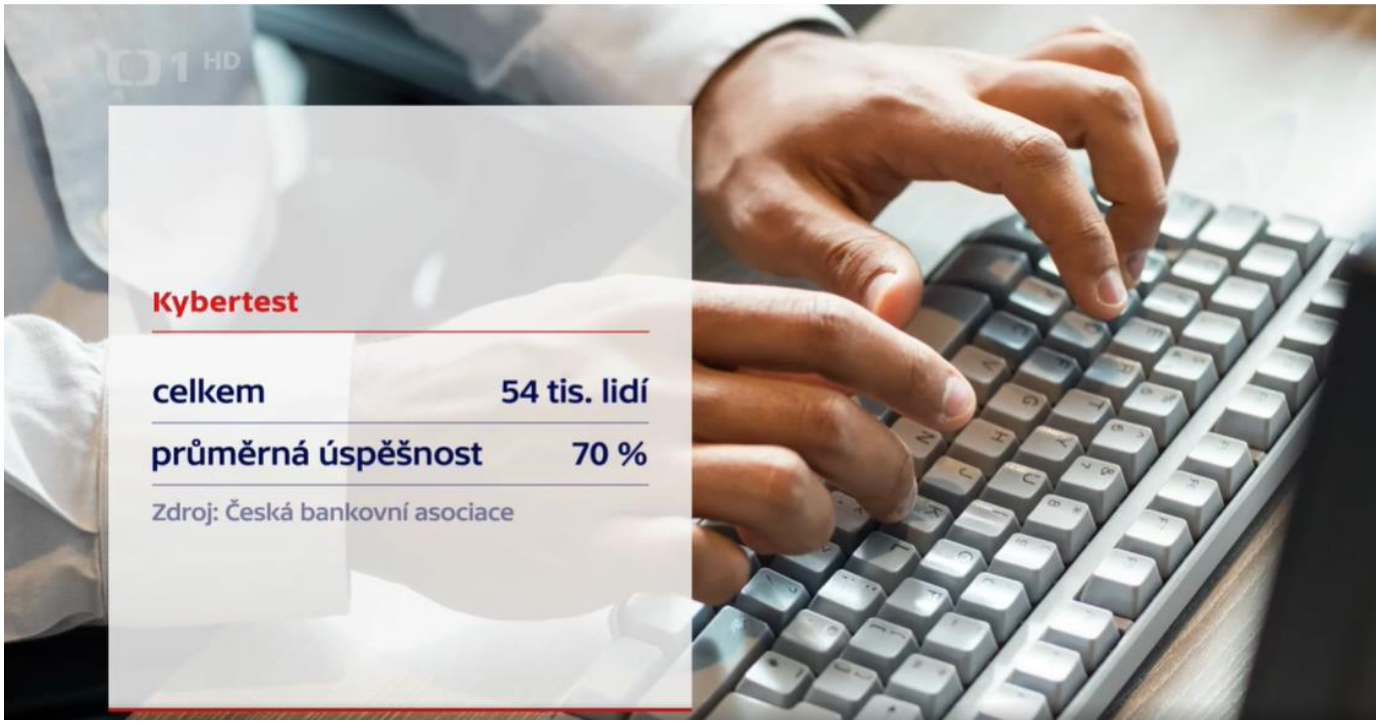
102. Kybergramotnost v Česku

Televize ● Události (ČT1) ● 25. 10. 2022, 19:27

Vydavatel: **ČESKÁ TELEVIZE (cz-00027383)**

Dosah: 651 166 ● GRP: 7.24 ● OTS: 0.07 ● AVE: 368234.37 Kč

Odkaz: náhled



103.Desítky lidí naletěly internetovým podvodníkům, škody jsou v milionech

Online ● novinky.cz (Zprávy / Politika) ● 26. 10. 2022, 8:34

Vydavatel: **BORGIS a.s. (cz-00564893)**

Dosah: 1 991 104 ● GRP: 22.12 ● OTS: 0.22 ● AVE: 45000.00 Kč ● Interakcí: 156

Odkaz: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-desitky-lidi-naletely-internetovym-podvodnikum-skody-jsou-v-milionech-40412717

Novinky.cz

Hlavní stránka Stalo se Domácí Volby Koronavirus Zahraniční Válka na Ukrajině Krimi Kultura Ek
Komentáře Internet a PC AutoMoto Muži Věda a školy Bydlení Cestování Historie Podcasty Spec

Novinky.cz » Internet a PC » Bezpečnost » Desítky lidí naletěly internetovým podvodníkům, škody jsou v mili

Desítky lidí naletěly internetovým podvodníkům, škody jsou v milionech

dnes 8:34 – Hradec Králové
Miloslav Fišer, Novinky, ČTK

Internetoví podvodníci připravili za uplynulý týden v Královéhradeckém kraji 29 lidí o téměř 13 milionů korun. Největší počet okradených, 15, klikl na zaslaný odkaz na falešné stránky bank. Téměř polovinu internetových podvodů z minulého týdne vyšetřují kriminalisté v okrese Hradec Králové, uvedla mluvčí policie Iva Kormošová.

Ilustrační foto

Čtyři lidi podvodníci připravili o peníze metodou, kdy se poškozený na sociálních sítích seznámí s neznámým cizincem, kterému pak na různé smyšlené účely posílá peníze. „Čtyři osoby zlákala nabídka investic a nainstalovaly si do počítače či telefonu program pro vzdálený přístup, tři lidé podlehli falešnému bankéři, který jim namluvil, že mají napadený účet. Tři lidé poslali předem peníze za inzerované zboží na bazarech," uvedla mluvčí.

Podle královéhradecké policie podvodníci v poslední době nejčastěji zasílají různé odkazy, kterými chtějí z lidí vylákat údaje z platební karty a přihlašovací údaje do internetového bankovnictví. „Podvodníci je zasílají pro potřeby uhrazení platby za zboží, kvůli přebukování doručovaného balíku, pro vyřízení sociální dávky, vrácení daní od finančního úřadu," uvedla mluvčí.

Při zatím posledním policii nahlášeném podvodu přišel ženě z Novobydžovska falešný e-mail z banky s aktivačním odkazem na takzvaný smart klíč. Žena na odkaz klikla a do bankovnictví se přihlásila. Následně jí z účtu odešly dvě platby v částce téměř 300 000 korun. Podvodný odkaz ženě přišel krátce poté, co z účtu platila oblečení nakoupené přes internet. Zda měla platba za oblečení souvislost s podvodným odkazem, policie vyšetřuje.

Milostní podvodníci tahali z lidí peníze. Ukořistili 20,5 milionu korun

Bezpečnost

Základní rady od policie, jak nenaletět internetovým podvodníkům

- Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, esemeska nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.
- Vyzkoušej si **www.kybertest.cz** a zjisti, kde máš mezery. Buď připraven.

104. Index Kyberbezpečnosti 2022 se drží na vysoké úrovni. Kybertestem prošly desítky tisíc lidí

Online ● casopisczechindustry.cz (Průmysl / Logistika) ● 27. 10. 2022, 21:23

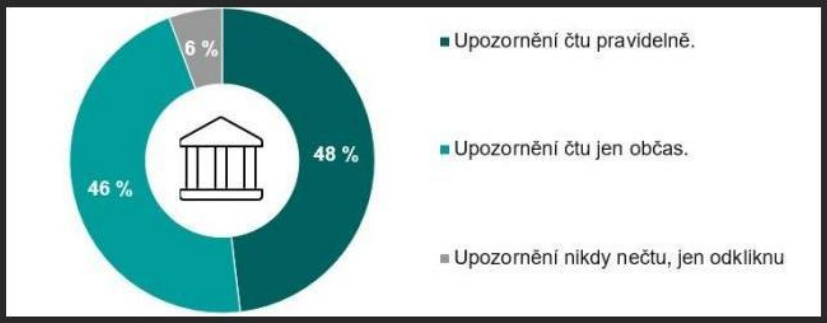
Vydavatel: **STUDIO P+P, s.r.o. (cz-25054562)**

Dosah: 667 ● GRP: 0.01 ● OTS: 0.00 ● AVE: 4327.53 Kč

Odkaz: https://www.casopisczechindustry.cz/products/index-kyberbezpecnosti-2022-se-drzi-na-vysoke-urovni-kybertestem-prosly-desitky-tisic-lidi/

Češi jsou ve sdílení informací opatrní, čtvrtina ale někdy otevře neznámou přílohu

Za žádných okolností by přihlašovací údaje k účtu neposkytlo 86 % Čechů. Víc než polovina by nesdílela ani výši svých úspor, číslo platební karty nebo rodinné fotografie. Další informace jsou lidé ochotni sdělit pouze za určitých okolností. Více než tři čtvrtiny se v takových případech podělí o telefonní číslo a adresu trvalého bydliště. Téměř tři čtvrtiny lidí neotvírají přílohy od neznámých odesílatelů, čtvrtina však alespoň některou otevře. Upozornění banky na možné hrozby čte většina lidí a přibližně polovina to dokonce dělá pravidelně. Osm z deseti Čechů se do svého internetového bankovnictví připojuje přes vlastní zařízení, které je zcela pod jejich kontrolou.



‚Česká populace je poměrně obezřetná v případě sdělování citlivých osobních údajůjako je číslo platební karty či přihlašovací údaje k bankovnímu účtu. Na druhou stranu však nemalá část lidí, přibližně čtvrtina, alespoň někdy otevírá přílohy emailů od neznámých uživatelů, což může způsobit vážný problém' uvádí Michal Straka z agentury Ipsos.

Bankám věří lidé v ochraně údajů nejvíc

Banky, pojišťovny či spořitelny jsou považovány za nejbezpečnější, co se týče ochrany před únikem dat. Za důvěryhodné je považuje 59 % Čechů. Oproti tomu státní správu (e-government) vnímá bezpečně pouze necelá třetina. Nejnižší důvěru mají u lidí fintech společnosti, nebankovní poskytovatelé půjček a obchodní řetězce.

Hackerských útoků přibývá, 27 % Čechů se s útokem setkalo letos

Víc než polovina Čechů se stala obětí hackerského útoku, a to bez ohledu na jeho dokončení. Třetina pak zná někoho, kdo byl obětí dokončeného útoku. Nejčastěji jde o podvodné e-maily, které slibují výhru v soutěži, popřípadě velké dědictví od zapomenutého člena rodiny. Víc než polovina má antivirový program v mobilním telefonu, u stolních počítačů je to sedm z deseti lidí. S útokem se nejčastěji setkávají lidé mezi 18 a 34 lety. 27 % Čechů se s útokem setkalo letos. Těmto údajům odpovídají i čísla České bankovní asociace. Počet útoků se za poslední dva roky zvýšil čtyřnásobně a průměrná škoda u dokončeného útoku je na jednoho klienta 162 tisíc korun. Útočníci nejčastěji cílí na získání přihlašovacích údajů, a to ve 40 % případů. Téměř třetina se pak snažila získat číslo platební karty a čtvrtina se zaměřila na osobní údaje, jako je například rodné číslo. Zájem byl také o heslo nebo PIN, a to ve 22 % případů.

Do elektronického bankovnictví se lidé nejčastěji připojují přes Wi-Fi

Lidé se přes Wi-Fi připojují pouze v případech, kdy je dobře zabezpečená. Ve zvyku to má 44 % z nich. Více než čtvrtina lidí se pak připojuje kdekoli, a to pomocí datového tarifu. Na veřejných sítích své finance spravuje pouze 8 % Čechů. Šest z deseti lidí je běžně používají na vyřizování svých e-mailů a jiné korespondence. Téměř polovina (44 %) se pak tímto způsobem přihlašuje na sociální sítě. „Připojovat se na veřejné, nezaheslované Wi-Fi není nikdy bezpečné. Nicméně lidé to dělají a budou dělat. Po připojení na veřejnou síť musí být lidé velmi ostražití a vstupovat do svého internetového či mobilního bankovnictví by vůbec neměli. Řada lidí si to ale stále neuvědomuje a kvůli tomu na sebe prozradí informace, které by prozrazovat neměli," říká Milan Habrcetl, Cyber Security Specialist společnosti Cisco.

Obchodování na on-line bazarech je časté, podvodné telefonáty lidé většinou odhalí

Téměř polovina Čechů někdy nakupovala na on-line bazarech a více než třetina na nich nějaké zboží prodávala. Nejčastější formou platby byl bankovní převod, ve čtyřech případech z deseti pak šlo o osobní předání. Podvodníci se často zaměřují právě na prodávající. Takových případů letos výrazně přibylo. „Protože jsou prodávající klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům nebo do jejich internetového bankovnictví. Aby co nejdříve docílili prodeje zboží, neopatrně spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně. Opak je bohužel pravdou, většinou o všechno přijdou" objasnil pplk. Ondřej Kapr z Policie ČR. Pouze 3 % lidí by poskytla informace při falešném telefonátu. Víc než polovina z nich by pak situaci ověřila u banky.

Kybertest si vyzkoušely desítky tisíc lidí, úspěšnost je v průměru 70 %

Česká bankovní asociace ve spolupráci s partnery v září spustila celonárodní kampaň #nePINDej!, která má za cíl přivést lidi na stránky Kybertest.cz a tímto způsobem je vzdělávat. Za necelé dva měsíce od spuštění Kybertestu kampaň přilákala téměř 54 tisíc lidí, kteří testem prošli v průměru se 70% úspěšností. Kybertest se skládá z deseti nejčastějších podvodů a lidé si tak mohou vyzkoušet, jak odolní jsou proti případným hackerským útokům. **ČBA nedávno spustila i obdobu Kybertestu pro mladší generaci**

Kyberhra.cz cílí na žáky druhého stupně základních škol, středních škol a odborných učilišť a víceletých gymnázií. Podvodníci si totiž své cíle vybírají napříč všemi generacemi, bez rozdílu věku či vzdělání. „V Thein Security si velmi dobře uvědomujeme sílu edukace v našem oboru. Šíření povědomí o bezpečném chování na internetu mezi běžné uživatele je to nejmenší, čím můžeme přispět. A přitom to nejzákladnější. Oceňujeme, že na problematiku upozorňují také silné společnosti, jako je právě Česká bankovní Asociace, jejíž aktivita má celostátní zásah napříč všemi věkovými skupinami. Těší nás, že jsme mohli být díky naší odbornosti v kybernetické bezpečnosti u tvorby Kybertestu a dosavadní pozitivní ohlasy nás ujišťují, že celá kampaň má skutečně velký smysl," říká Jan Pinta, kyberbezpečnostní expert Thein Security. Mladiství jsou snadným cílem podvodníků také proto, že se v kyberprostoru pohybují velmi často. Mají chytrá zařízení, ale přesně nevědí, jak se v on-line prostředí bezpečně chovat. (27.10.2022)

105. „Váš účet byl napaden.“ Podvodným telefonátům podlehne každý druhý

Online ● seznamzpravy.cz (Zprávy / Politika) ● 29. 10. 2022, 8:49

Vydavatel: **Seznam.cz, a.s. (cz-26168685)** ● Autor: **Karolína Štuková**

Dosah: 1 702 492 ● GRP: 18.92 ● OTS: 0.19 ● AVE: 79177.75 Kč ● Interakcí: 377

Odkaz: https://www.seznamzpravy.cz/clanek/ekonomika-finance-vas-ucet-byl-napaden-podvodnym-telefonatum-podlehne-kazdy-druhy-217833

Ilustrační foto.

8:49

„Zjistili jsme na vašem účtu podvod“ nebo „Budu potřebovat údaje o vaší kartě“. Tak začíná podvod, který může stát podvedeného klienta banky statisíce korun. Počet případů roste.

Článek si také můžete poslechnout v audioverzi.

Zvoní telefon a z neznámého čísla se na druhém konci představí falešný úředník, bankéř, finanční poradce nebo dokonce policista. Už za několik vteřin ale přichází otázka, která může potenciální oběť podvodného telefonátu stát peníze, které šetřila roky.

Případů podvodného navolávání, z angličtiny takzvaného vishingu, každoročně roste. Podle informací Policie ČR kriminalisté zaznamenávají případy podvodů i s milionovými škodami.

Falešný e-mail nebo odkaz v SMS. Podvod stojí jednoho člověka desetitisíce

13. 10. 17:38

„Podvody jsou často založeny na principu telefonních hovorů, kdy se volající představí jako pracovník banky, který zjistil napadení účtu volaného. Fiktivní bankovní úředník vystraší různými tvrzeními osobu, které volá, a přiměje jí peníze z účtu převést na bankovní účet, který označí jako bezpečný. Tvrdí přitom, že se jedná pouze o dočasné bezpečnostní opatření. Věrohodnost pokynů fiktivního bankovního úředníka umocňuje často další telefonát, tentokrát osoby vydávající se za policistu. Ten potvrzuje volanému tvrzení uvedená v prvním telefonátu a nezbytnost převedení peněz na bezpečnější účet," vysvětluje princip podvodu mluvčí policejního prezidia Jakub Vinčálek.

Tvrzení podvodníků bývají navíc velmi věrohodná. Často předem disponují informací o skutečné bankovní instituci, ve které má volaný svůj účet. K tomu využívají takzvaného spoofingu telefonního čísla, což znamená, že dokážou napodobit jakékoliv telefonní číslo, tedy i infolinku banky. Kromě peněz získávají podvodníci také citlivé osobní údaje, které mohou kdykoliv zneužít.

Kampaň #nePINdej!

Patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti u nás. Zapojily se jak orgány státní správy, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají.

Kromě ČBA i Policie České republiky, Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), itego, a. s., Cisco, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy.

Mediálními partnery jsou Česká televize (hlavní mediální partner), Seznam Zprávy, Deník a CineStar.

„Nárůst v posledním desetiletí souvisí s rozvojem informačních a komunikačních

technologií i zvyšujícím se počtem uživatelů. Této situace zcela jasně začali zneužívat i pachatelé různých forem trestné činnosti, kterým online prostředí slouží bohužel jako nástroj pro páchání trestné činnosti," vysvětluje Vinčálek pro SZ Byznys.

Pachatelům za jejich jednání podle slov mluvčího policejního prezidia hrozí trest odnětí svobody až osm let.

Právě vishingových útoků v posledních letech přibývá zejména v oblasti bankovnictví.

„Útoků na klienty bank přibývá v posledních dvou letech mnohanásobně a každý den banky řeší desítky takovýchto případů, přičemž počet i škoda se na konci letošního roku dá odhadovat na dvojnásobek toho, co banky zaznamenaly v roce 2021," uvedl Petr Barák, předseda Komise bankovní a finanční bezpečnosti České bankovní asociace.

Problém je navíc i to, že se zvyšuje úspěšnost útoků. Téměř každý druhý podvodný telefonát v současné době končí škodou pro klienta. Průměrná částka, o kterou klienti při vishingových útocích přijdou, se na jednoho klienta pohybuje kolem 250 tisíc korun, ukazují data ČBA.

Důvodem je podle jeho slov fakt, že se bankovní odvětví za poslední dva roky výrazně přesunulo do virtuálního světa a klienti bohužel stále nevnímají všechna jeho rizika.

Podle Bartáka mimo jiné pachatelům napomáhá současná ekonomická situace, protože jimi vytvořené podvodné scénáře jsou pro klienty bank zajímavé. Například vysoká inflace tlačí klienty bank k tomu, aby své peníze nenechávali jen na účtech v bankách, kde se jejich hodnota s ohledem na rozdíl mezi úrokovými sazbami a výší inflace znehodnocuje.

Pravidla pro bezpečné chování v kyberprostoru:

- Pokud potřebuji řešit něco s bankou, vždy se na ni obracím sám.

- Ctu, co mi banka posílá, a slepě neklikám jen na odkazy, které mi přijdou do e-mailu nebo mobilu.
- Nesděluji citlivé bankovní informace do telefonu někomu, kdo se mi představí jako pracovník banky, když nevím, že opravdu z banky volá a neumím si to ověřit .
- Nevyplňuji citlivé informace na neznámých stránkách (byť se mohou tvářit jako stránky banky), tedy například kontroluji jejich webové adresy a všímám si, co je v nich napsáno a kdo je jejich provozovatelem, včetně země, kde jsou vytvořeny.
- Říká se i to, že bych neměl věřit tomu, co se tváří jako až příliš hezké na to, aby to skutečně byla pravda.
- Zdroj: Kybertest.cz

Podvodná praktika falešných telefonátů je ale jen jednou z mnoha dalších, se kterými se běžný uživatel může v online prostředí setkat. Další významnou součástí jsou investiční podvody, respektive podvodná jednání s legendou investice, především do kryptoměn.

Pachatelé často využívají internetové reklamy na sociálních sítích a dalších platformách a často připravují velmi kvalitně, téměř profesionálně zpracované webové stránky prezentující jejich podvodnou platformu.

Setrvalým problémem je také klasický tzv. phishing ve všech formách, jako jsou falešné e-maily nebo textové zprávy. Mezi další z nich patří také inzertní podvody, reverzní inzertní podvody, kdy se obětí naopak stává prodávající, a registrován je i nárůst případů podvodných platebních bran.

S nejčastějšími podvodnými útoky se můžete seznámit níže.

Nejčastější podvodné útoky v online prostředí:

1) Podvodné telefonáty o napadení bankovního účtu

Pachatel se v podvodném telefonátu vydává za vašeho bankéře, který vás z důvodu napadení vašeho účtu přiměje k přeposlání finančních prostředků na „bezpečný“ účet, či k vložení peněz v hotovosti do vkladomatu na virtuální měny.

2) Umožnění vzdáleného přístupu do vašeho zařízení

Pachatel se z vás pod různými legendami snaží vylákat přístup do vašeho mobilního telefonu či počítače. Vmanipuluje vás do instalace softwaru pro vzdálený přístup s jediným cílem. Dostat se vzdáleně do vašeho bankovnictví a odcizit všechny vaše úspory, včetně finančních prostředků z půjček, co si na vás po získání přístupů sjedná.

3) Prodeje na inzertních serverech

Pachatel zareaguje na váš inzerát se zájmem o zboží, které chcete prodávat. Falešný zájemce se vás v rámci urychlení a zjednodušení obchodu snaží přesvědčit ke vložení citlivých údajů o vašem bankovnictví do platební brány, která se na první pohled může zdát jako pravá. Následně vámi sdílené údaje zneužije. Jedná se především o číslo vaší karty, datum expirace, CVV/CVC kód a pin.

4) Podvodné phishingové kampaně prostřednictvím SMS zpráv, e-mailů či sociálních sítí

Každý den pachatelé rozesílají velké množství podvodných e-mailů, SMS zpráv či zpráv přes sociální sítě a snaží se vás nalákat na různé legendy. Často to je zabezpečení vašich účtů, zásilka zboží, daňový přeplatek, či nedoplatek, aktualizace zabezpečení apod.

5) Kamarád píše přes sociální sítě, protože ztratil vaše telefonní číslo

5) Kamarád píše přes sociální sítě, protože ztratil vaše telefonní číslo

Pachatel vás kontaktuje jménem vašeho přítele nebo přímo z profilu vašeho přítele. Často požaduje vaše telefonní číslo, buď ho ztratil, nebo vás přihlásil do soutěže, nebo vám posílá nějaký benefit. Následně vás požádá o zaslání ověřovacího kódu, aby transakci dokončil. Kód zneužije a okrade vás na mobilních platbách, případně zneužije i váš profil na sociální síti k zasílání podvodných zpráv i vašim přátelům.

6) Požadavek přeposlání peněz přes váš bankovní účet

Nabídka výhodné brigády, snaha pomoci kamarádovi či vaše neopatrnost může pachatelům umožnit převádět přes váš účet finanční prostředky pocházející z různých podvodů. Pachatelé často nabízejí různé možnosti přivýdělku, které se na první pohled tváří jako zcela legální.

7) Zázračné zbohatnutí skrze výhodné investice

Zaujala vás reklama na výhodnou a zcela bezpečnou investici s téměř astronomickým ziskem? Zbohatly takto i veřejně známé osobnosti, které výhodnost investice v komentářích potvrzují? Obvykle se jedná o podvod. Falešní investoři vás prvoplánově chtějí okrást o částku, kterou jim sami zašlete, nebo se vám chtějí dostat do vašeho zařízení přes vzdálený přístup a získat přístupy do vašeho bankovnictví, kde si již převody provedou sami.

8) Podvody založené na lásce a zázračném zbohatnutí

Pachatelé vás kontaktují obvykle prostřednictvím seznamovacích portálů pod různými identitami (např. americký voják, letec, doktor, dělník na ropné věži, právník) a snaží se vás zmanipulovat. Podvody jsou často založené na zaslání nějaké cenné zásilky (zlatý poklad, neočekávaná výhra, peníze z dědictví atd.). Vždy se po cestě zásilky najde nějaký zádrhel, který musíte vyřešit zaplacením poplatku, jenž se postupně vyšplhá až na miliony, které už nikdy neuvidíte.

Zdroj: Policie ČR

Jak jsou na tom vaše znalosti základních principů bezpečného chování na internetu, si můžete vyzkoušet v online interaktivním kybertestu, který v rámci vzdělávací kampaně spustila Česká bankovní asociace.

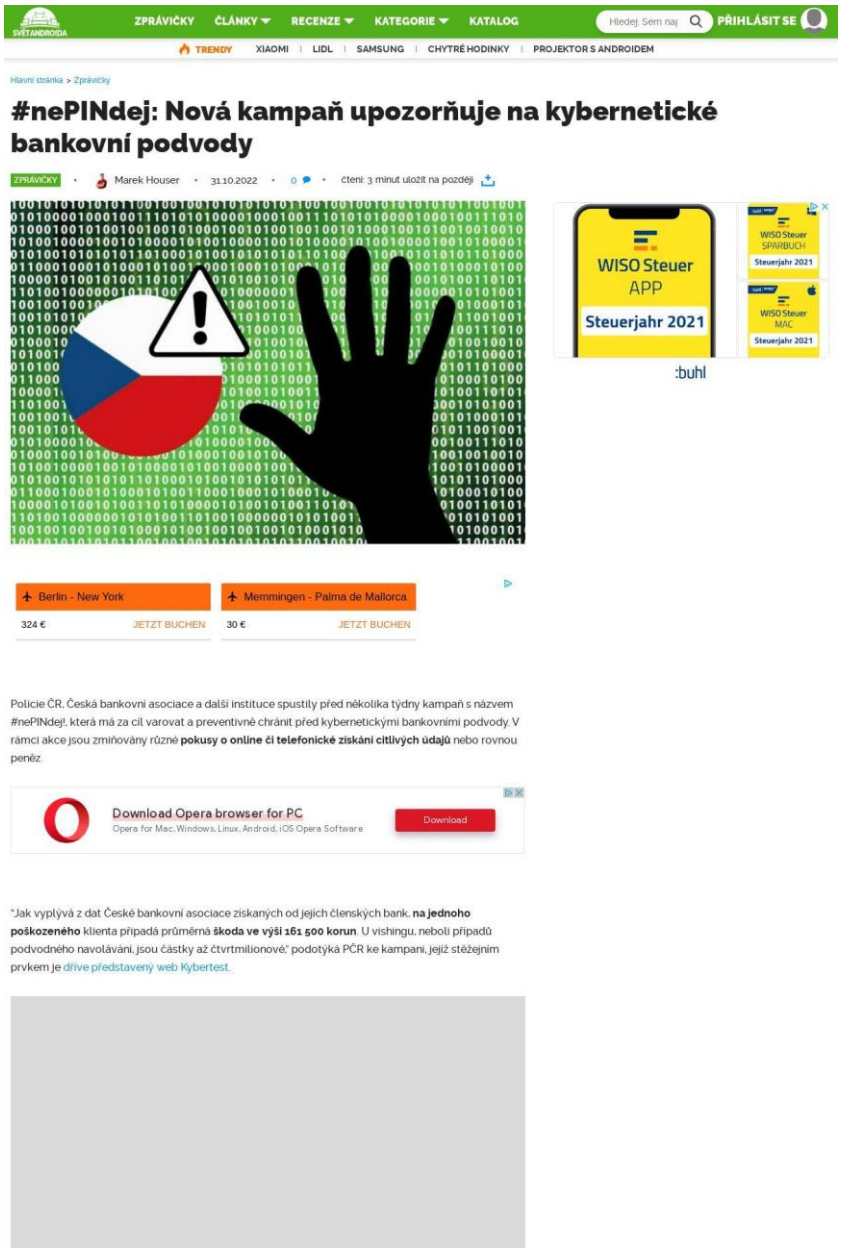
106. #nePINdej: Nová kampaň upozorňuje na kybernetické bankovní podvody

Online ● svetandroida.cz (IT / Technologie) ● 31. 10. 2022, 20:00

Vydavatel: **Svět Zítřka s.r.o. (cz-04778863)** ● Autor: **Marek Houser** ● Rubrika: **Zprávičky**

Dosah: 48 779 ● GRP: 0.54 ● OTS: 0.01 ● AVE: 27358.67 Kč

Odkaz: https://www.svetandroida.cz/nepindej-kampan-kyberneticke-bankovni-podvody/



Podvody, které nejen v ČR frčí:

- **Podvodné navolávání (vishing)** – Pachatelé se vydávají například za bankéře, policisty, pracovníky technické podpory a snaží se z lidí pod vlivem strachu vylákat peníze, nebo vzdálený přístup do zařízení oběti, který následně zneužije.
- **Nabídka výhodných investic –** Přesvědčivá lákavá reklama a manipulativní jednání. Cílem pachatele je vylákat z oběti co možná nejvíce finančních prostředků a využívá k tomu přirozenou ziskuchtivost každého z nás.
- **Reverzní inzertní podvody** – Pachatel zareaguje na váš inzerát. Podstrčí vám fiktivní platební bránu, kde vyplníte citlivé bankovní údaje a místo peněz za inzerované zboží přicházíte o všechny úspory.
- **Podvody typu Nigerijské dopisy** – Princip, který funguje už více jak 100 let. Pachatelé sázejí na kvantitu. Vždy se najde někdo, kdo se nechá nachytat na slibovanou cennou zásilku nebo domnělou pomoc. Často zde hraje velkou roli láska.
- **Klasické podvody typu phishing a smishing** – Stále dokonalejší a složitě rozpoznatelné podvodné emaily a SMS nabídky. Na první pohled již nenajdeme podezřelé znaky.

Policie rovněž upozorňuje, že kromě tradičních podvodných e-mailů, SMS a již zmíněného vishingu se stále častěji setkává s podvody na sociálních sítích, kdy pachatel může dokonce **ukrást identitu reálné osoby** a pod ní pak kontaktovat její přátele s cílem vylákat z nich peníze.

Tyto aplikace z Google Play umí vysát účet. Zbavte se jich

ZPRÁVIČKY Marek Houser

Základní rady, jak nenaletět

- Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.
- Vyzkoušej si www.kybertest.cz a zjisti, kde máš mezery. Buď připraven.

Kyberkampaň #nePINdej! bude s ohledem na širokou cílovou skupinu probíhat napříč všemi médii – na internetu, v tisku, v České televizi, využita bude i tištěná reklama – formou letáků na pobočkách České pošty –, a pevné reklamní plochy ve vlacích a na nádražích Českých drah, ale **i na bankomatech bank** působících na českém trhu. Společnost O2 pak kampaň podpoří SMS zprávami s výzvou k účasti na testu.

Ze sociálních sítí bude kromě standardních kanálů (Facebook, LinkedIn, Twitter, Instagram) nově využit i TikTok. Kampaň podpoří na svých profilech i influencer Martin „Mikýř" Mikyska.

Kde už jste se setkali s kampaní #nePINdej?

Foto: kalhh

107. ČBA NEWS

Tisk ● ČBA News; str. 1 (Ekonomika / Finance / Právo) ● 1. 11. 2022

Autor: **Monika Zahálková**

Odkaz: náhled

22/2022 For English version please click here.

ČESKÁ BANKOVNÍ ASOCIACE CZECH BANKING ASSOCIATION NEWS

Milé kolegyně, milí kolegové,

není žádným tajemstvím, že Česká bankovní asociace považuje kyberbezpečnost za jedno z nejaktuálnějších témat, kterému se intenzivně věnuje. Již mnohokrát jsme vás informovali o právě probíhající kampani #nePINdej!, která je na svém pomyslném vrcholu a nově se s ní můžete setkat i na televizních obrazovkách. Díky partnerství s Českou televizí máme možnost v hlavním vysílacím čase odvysílat spoty varující před kybernetickými podvodníky a propagující náš Kybertest. Ten si v současné době vyzkouší denně více než 1800 lidí, což považujeme za skvělé číslo. Uspokojivý je i výsledek, se kterým zájemci test dokončí. V průměru se skóre pohybuje kolem 70 %. Není to špatné, ale nenalhávejme si, že je to dobré. V kyberprostoru totiž stačí jen malá nepozornost a vaše úspory jsou nenávratně pryč.
Také proto kyberbezpečnosti věnujeme v dnešním vydání nemalý prostor. V našem každoročním průzkumu jsme opět změřili Index kyberbezpečnosti, který je letos o malinko horší než loni. O tom, jak se Češi pohybují v online světě, jak si chrání svá zařízení a jaká používají nejčastější hesla, se můžete dočíst v rubrice Téma.

Přeji vám příjemné čtení a klidný podzim.

Monika Zahálková, výkonná ředitelka

108. Index Kyberbezpečnosti 2022: Češi jsou v on-line prostoru bank stále opatrní

Tisk ● ČBA News; str. 7 (Ekonomika / Finance / Právo) ● 1. 11. 2022

Odkaz: náhled

Index Kyberbezpečnosti 2022: Češi jsou v on-line prostoru bank stále opatrní

Češi jsou v online prostoru obezřetní. Index Kyberbezpečnosti dosáhl 67 bodů a drží se tak blízko výsledku z loňského roku. Finanční operace lidé považují za citlivé a k internetovému či mobilnímu bankovnictví by nikdy neposkytla přístup většina z nich. Banky jsou pro Čechy nejdůvěryhodnější instituce, pokud jde o ochranu před únikem dat. Vyplývá to z průzkumu České bankovní asociace a výzkumné agentury Ipsos. Výsledkům průzkumu odpovídají i průběžná data Kybertestu, kterým během necelých dvou měsíců prošlo 82 tisíc lidí s průměrným výsledkem 70 %.

Index Kyberbezpečnosti dosáhl 67 bodů, o jeden bod méně než loni

V loňském roce byly výsledky nejlepší od začátku sledování, index dosáhl 68 %. Lidé se základním vzděláním získali v průměru 65 %, zatímco vysokoškolsky vzdělaní dostali průměrně 68 %. *„Zdá se, že lidé si uvědomují rizika, která jsou s online prostředím spojená. Naprostá většina by neposkytla přístupové údaje do internetového bankovnictví. Téměř dvě třetiny lidí kontrolují výdaje a úspory na účtu pravidelně,"* říká Petr Barák, expert České bankovní asociace na finanční a bankovní bezpečnost.

Češi jsou ve sdílení informací opatrní, čtvrtina ale někdy otevře neznámou přílohu

Za žádných okolností by přihlašovací údaje k účtu neposkytlo 86 % Čechů. Více než polovina by nesdílela ani výši svých úspor, číslo platební karty nebo rodinné fotografie. Další informace jsou lidé ochotni sdělit pouze za určitých okolností. Více než tři čtvrtiny se v takových případech podělí o telefonní číslo a adresu trvalého bydliště. Téměř tři čtvrtiny lidí neotvírají přílohy od neznámých odesílatelů, čtvrtina však alespoň některou otevře. Upozornění banky na možné hrozby čte většina a přibližně polovina to dokonce dělá pravidelně. Osm z deseti Čechů se do svého internetového bankovnictví připojuje přes vlastní zařízení, které je zcela pod jejich kontrolou.

109. Kybertest si vyzkoušely desítky tisíc lidí, úspěšnost je v průměru 70 %

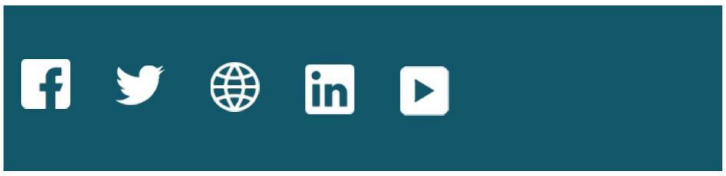
Tisk ● ČBA News; str. 9 (Ekonomika / Finance / Právo) ● 1. 11. 2022

Odkaz: náhled

situaci ověřila u banky.

Kybertest si vyzkoušely desítky tisíc lidí, úspěšnost je v průměru 70 %

Česká bankovní asociace ve spolupráci s partnery v září spustila celonárodní kampaň #nePINDej!, která má za cíl přivést lidi na stránky Kybertest.cz a tímto způsobem je vzdělávat. Za necelé dva měsíce od spuštění Kybertestu kampaň přilákala téměř 82 tisíc lidí, kteří testem prošli v průměru se 70% úspěšností. Kybertest se skládá z deseti nejčastějších podvodů a lidé si tak mohou vyzkoušet, jak odolní jsou proti případným hackerským útokům. ČBA nedávno spustila i obdobu Kybertestu pro mladší generaci. Kyberhra.cz cílí na žáky druhého stupně základních škol, středních škol a odborných učilišť a víceletých gymnázií. Podvodníci si totiž své cíle vybírají napříč všemi generacemi, bez rozdílu věku či vzdělání.



110. ČBA: „Index Kyberbezpečnosti 2022 se drží na vysoké úrovni“

Online ● sos-msk.cz (Jiné) ● 1. 11. 2022, 8:00

Vydavatel: **Sdružení obrany spotřebitelů Moravy a Slezska, z.s. (cz-22831738)** ● Rubrika: **Svět kolem nás**

Dosah: 56 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 1036.42 Kč

Odkaz: https://www.sos-msk.cz/cba-index-kyberbezpecnosti-2022-se-drzi-na-vysoke-urovni/

ČBA: „Index Kyberbezpečnosti 2022 se drží na vysoké úrovni“

autor: SOS MaS | Lis 1, 2022 | Svět kolem nás | 0 komentářů

Index Kyberbezpečnosti 2022 se podle výzkumu České bankovní asociace drží na vysoké úrovni. Kybertestem prošly desítky tisíc lidí.

Češi jsou v online prostoru opatrní. Index Kyberbezpečnosti dosáhl 67 bodů a drží se tak blízko výsledku z loňského roku. Finanční operace lidé považují za citlivé a k internetovému či mobilnímu bankovnictví by nikdy neposkytla přístup většina z nich. Banky jsou pro Čechy nejdůvěryhodnější instituce, pokud jde o ochranu před únikem dat. Vyplývá to z průzkumu České bankovní asociace a výzkumné agentury Ipsos. Výsledkům průzkumu odpovídají i průběžná data Kybertestu, kterým během necelých dvou měsíců prošlo 54 tisíc lidí s průměrným výsledkem 70 %.

Index Kyberbezpečnosti dosáhl 67 bodů, o jeden bod méně než loni.

V loňském roce byly výsledky nejlepší od začátku sledování, index dosáhl 68 bodů. Letos je výsledek jen nepatrně

nižší. Výsledky jsou z různých hledisek velmi vyrovnané. Lidé se základním vzděláním získali v průměru 65 bodů, zatímco vysokoškolsky vzdělaní získali průměrně 68 bodů.

„Zdá se, že lidé si uvědomují rizika, která jsou s online prostředím spojená. Naprostá většina by neposkytla přístupové údaje do internetového bankovnictví. Téměř dvě třetiny lidí kontrolují výdaje a úspory na účtu pravidelně," říká **Petr Barák**, expert České bankovní asociace na finanční a bankovní bezpečnost.

Češi jsou ve sdílení informací opatrní, čtvrtina ale někdy otevře neznámou přílohu

Za žádných okolností by přihlašovací údaje k účtu neposkytlo 86 % Čechů. Víc než polovina by nesdílela ani výši svých úspor, číslo platební karty nebo rodinné fotografie. Další informace jsou lidé ochotni sdělit pouze za určitých okolností. Více než tři čtvrtiny se v takových případech podělí o telefonní číslo a adresu trvalého bydliště. Téměř tři čtvrtiny lidí neotvírají přílohy od neznámých odesílatelů, čtvrtina však alespoň některou otevře. Upozornění banky na možné hrozby čte většina lidí a přibližně polovina to dokonce dělá pravidelně. Osm z deseti Čechů se do svého internetového bankovnictví připojuje přes vlastní zařízení, které je zcela pod jejich kontrolou.

„Česká populace je poměrně obezřetná v případě sdělování citlivých osobních údajů jako je číslo platební karty či přihlašovací údaje k bankovnímu účtu. Na druhou stranu však nemalá část lidí, přibližně čtvrtina, alespoň někdy otevírá přílohy emailů od neznámých uživatelů, což může způsobit vážný problém" uvádí **Michal Straka** z agentury Ipsos.

Bankám věří lidé v ochraně údajů nejvíc

Banky, pojišťovny či spořitelny jsou považovány za nejbezpečnější, co se týče ochrany před únikem dat. Za důvěryhodné je považuje 59 % Čechů. Oproti tomu státní správu (e-government) vnímá bezpečně pouze necelá třetina. Nejnižší důvěru mají u lidí fintech společnosti, nebankovní poskytovatelé půjček a obchodní řetězce.

Hackerských útoků přibývá, 27 % Čechů se s útokem setkalo letos

Víc než polovina Čechů se stala obětí hackerského útoku, a to bez ohledu na jeho dokončení. Třetina pak zná někoho, kdo byl obětí dokončeného útoku. Nejčastěji jde o podvodné e-maily, které slibují výhru v soutěži, popřípadě velké dědictví od zapomenutého člena rodiny. Víc než polovina má antivirový program v mobilním telefonu, u stolních počítačů je to sedm z deseti lidí. S útokem se nejčastěji setkávají lidé mezi 18 a 34 lety. 27 % Čechů se s útokem setkalo letos. Těmto údajům odpovídají i čísla České bankovní asociace. Počet útoků se za poslední dva roky zvýšil čtyřnásobně a průměrná škoda u dokončeného útoku je na jednoho klienta 162 tisíc korun. Útočníci nejčastěji cílí na získání přihlašovacích údajů, a to ve 40 % případů. Téměř třetina se pak snažila získat číslo platební karty a čtvrtina se zaměřila na osobní údaje, jako je například rodné číslo. Zájem byl také o heslo nebo PIN, a to ve 22 % případů.

Pouze 3 % lidí by poskytla informace při falešném telefonátu. Víc než polovina z nich by pak situaci ověřila u banky.

Kybertest si vyzkoušely desítky tisíc lidí, úspěšnost je v průměru 70 %

Česká bankovní asociace ve spolupráci s partnery v září spustila celonárodní kampaň #nePINDej! která má za cíl přivést lidi na stránky Kybertest.cz a tímto způsobem je vzdělávat. Za necelé dva měsíce od spuštění Kybertestu kampaň přilákala téměř 54 tisíc lidí, kteří testem prošli v průměru se 70% úspěšností. Kybertest se skládá z deseti nejčastějších podvodů a lidé si tak mohou vyzkoušet, jak odolní jsou proti případným hackerským útokům.

Do elektronického bankovnictví se lidé nejčastěji připojují přes Wi-Fi

Lidé se přes Wi-Fi připojují pouze v případech, kdy je dobře zabezpečená. Ve zvyku to má 44 % z nich. Více než čtvrtina lidí se pak připojuje kdekoli, a to pomocí datového tarifu. Na veřejných sítích své finance spravuje pouze 8 % Čechů. Šest z deseti lidí je běžně používají na vyřizování svých e-mailů a jiné korespondence. Téměř polovina (44 %) se pak tímto způsobem přihlašuje na sociální sítě.

„Připojovat se na veřejné, nezaheslované Wi-Fi není nikdy bezpečné. Nicméně lidé to dělají a budou dělat. Po připojení na veřejnou síť musí být lidé velmi ostražití a vstupovat do svého internetového či mobilního bankovnictví by vůbec neměli. Řada lidí si to ale stále neuvědomuje a kvůli tomu na sebe prozradí informace, které by prozrazovat neměli," říká **Milan Habrcetl**, Cyber Security Specialist společnosti Cisco.

Obchodování na on-line bazarech je časté, podvodné telefonáty lidé většinou odhalí

Téměř polovina Čechů někdy nakupovala na on-line bazarech a více než třetina na nich nějaké zboží prodávala. Nejčastější formou platby byl bankovní převod, ve čtyřech případech z deseti pak šlo o osobní předání. Podvodníci se často zaměřují právě na prodávající. Takových případů letos výrazně přibylo.

„Protože jsou prodávající klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům nebo do jejich internetového bankovnictví. Aby co nejdříve docílili prodeje zboží, neopatrně spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně. Opak je bohužel pravdou, většinou o všechno přijdou" objasnil **pplk. Ondřej Kapr** z Policie ČR.

Pouze 3 % lidí by poskytla informace při falešném telefonátu. Víc než polovina z nich by pak situaci ověřila u banky.

Kybertest si vyzkoušely desítky tisíc lidí, úspěšnost je v průměru 70 %

Česká bankovní asociace ve spolupráci s partnery v září spustila celonárodní kampaň #nePINDej! která má za cíl přivést lidi na stránky Kybertest.cz a tímto způsobem je vzdělávat. Za necelé dva měsíce od spuštění Kybertestu kampaň přilákala téměř 54 tisíc lidí, kteří testem prošli v průměru se 70% úspěšností. Kybertest se skládá z deseti nejčastějších podvodů a lidé si tak mohou vyzkoušet, jak odolní jsou proti případným hackerským útokům.

ČBA nedávno spustila i obdobu Kybertestu pro mladší generaci. Kyberhra.cz cílí na žáky druhého stupně základních škol, středních škol a odborných učilišť a víceletých gymnázií. Podvodníci si totiž své cíle vybírají napříč všemi generacemi, bez rozdílu věku či vzdělání.

„V Thein Security si velmi dobře uvědomujeme sílu edukace v našem oboru. Šíření povědomí o bezpečném chování na internetu mezi běžné uživatele je to nejmenší, čím můžeme přispět. A přitom to nejzákladnější. Oceňujeme, že na problematiku upozorňují také silné společnosti, jako je právě Česká bankovní Asociace, jejíž aktivita má celostátní zásah napříč všemi věkovými skupinami. Těší nás, že jsme mohli být díky naší odbornosti v kybernetické bezpečnosti u tvorby Kybertestu a dosavadní pozitivní ohlasy nás ujišťují, že celá kampaň má skutečně velký smysl," říká Jan Pinta, kyberbezpečnostní expert Thein Security.

Mladiství jsou snadným cílem podvodníků také proto, že se v kyberprostoru pohybují velmi často. Mají chytrá zařízení, ale přesně nevědí, jak se v on-line prostředí bezpečně chovat.

Zdroj: Česká bankovní asociace, www.cba.cz. Tisková zpráva dostupná on-line: https://cbaonline.cz/upload/2424-tz-index-kyberbezpecnosti-2022-a-kybertest.pdf

111. SMS nebo e-mail. Zprávy, které lidi připravují o úspory

Tisk ● Tachovský deník; str. 6 (Regionální zprávy) ● 3. 11. 2022

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)**

Dosah: 542 613 ● GRP: 6.03 ● OTS: 0.06 ● AVE: 989352.97 Kč

Odkaz: náhled

UDÁLOSTI

Komentář

Martin KOMÁREK
šéfkomentátor

Horká válka o Kavčí hory

Válka o televizi přešla do horké fáze. Zatím se vede naštěstí jen ústy, obě strany však používají slovní kanony nejtěžšího kalibru.

Koalice protlačila prvním čtením novelu zákona o České televizi a Českém rozhlasu. V čem spočívají změny? Do volby rad, tedy jakýchsi výborů, jejichž výsostným právem je volit ředitele a kontrolovat hospodaření veřejnoprávních médií, se zapojí i Senát. Dosud členy volila Poslanecká sněmovna. Radní nepůjde odvolat tak snadno jako doposud. Hezké?

Opozice křičí z pláně hrdla: Je to podraz! V Senátu totiž nemá sílu, a je tedy zřejmé, že tam projdou kandidáti blízcí vládě. Ta tak bude mít rozhodující vliv na volbu nového ředitele televize. Opravdu? Správně by měli politici volit nezávislé odborníky. Skutečnost je však jiná. Zejména poslanci jsou televizním zpravodajstvím posedlí. A dělají vše pro to, aby si je podmanili.

„Poslanci jsou televizním zpravodajstvím posedlí. A dělají vše pro to, aby si je podmanili."

Z formálního hlediska jsou naše veřejnoprávní média zcela nezávislá. Rady se nemusejí nikomu zodpovídat a řídí se svou úvahou. Český rozhlas a televize nejsou placeny ze státního rozpočtu, ale občany. Vláda tedy nemůže na jejich peníze sáhnout a ani do ničeho mluvit.

Na tom, kdo televizi platí a jak jsou voleni radní, však tolik nezáleží. Spíš na zvykovém právu. V starších unijních zemích jsou politici zdrženliví, svobodu médií považují za něco samozřejmého. U nás jsou zejména na Českou televizi naježení. Redaktoři čelí často nátlaku.

Ale zpět k té směnovní válce. Vládní poslanci jsou možná zčásti vedeni bohulibými úmysly. Touha zvýšit vliv na ČT jim ale srší z očí. Už v červnu kvůli tomu prosadili volbu členů rady veřejným hlasováním. To je sice možné, ale zcela mimořádné. Podle parlamentních zvyklostí jsou všechny personální volby tajné. Kdyby něco takového udělal Andrej Babiš, když byl u moci, statisíce lidí by vyšly do ulic.

I nynější změna zákona se zdá být účelovou. Pokud se tedy opozice brání do statků a hrdel, činí správně.

Už zítra v Deníku

Benda: Chtěl jsem na Hrad vlastního kandidáta ODS

Praha – Matador české politiky a šéf poslaneckého klubu ODS Marek Benda měl vlastní favority na prezidentské kandidáty. „Byli to Alexandr Vondra, Miloš Vystrčil, Mirka Němcová a další. „Nakonec mi všichni řekli, že jím to za to nestojí. Bude to – a v okamžiku, kdy se Andrej Babiš rozhodl kandidovat, už je to jasné – strašně krutě. Budou se prověřovat babičky do sedmého a vnoučata do třetího kolene," řekl Deníku. V rozhovoru také hovoří o tom, proč je citlivý na zákonné umlčování dezinformátorů a nálepkování nositelů jiných názorů. **(kp)**

rozhovor Kateřiny Perknerové

A proč se nedaří sestavit pražskou koalici? Dočtete se v zítřejším vydání Deníku.

Víte, že?

Deník pořídá už skoro deset let. Kabelkový veletrh, jehož výtěžek jen v jižních Čechách byl celkem 1,4 milionu korun.

Načtěte tento kód svým mobilním telefonem.

www.denik.cz/odeniku

SMS nebo e-mail. Zprávy, které lidi připravují o úspory

Pozor na podvodné SMS a e-mailové zprávy. Podvodníci se snaží ukrást úspory. Nový seriál Deníku Digitální podvody radí, jak se vyhnout ztrátě peněz či osobních údajů na internetu.

Digitální podvody
Jak bránit své peníze

VILÉM JANOUŠ

Máte nedoplatek, který je potřeba ihned uhradit, oznámila jednačtyřicetiletému Jiřímu SMS. Tvářila se jako oficiální zpráva finančního úřadu a rovnou obsahovala odkaz na platbu. „Nechtěl jsem mít žádné problémy, tak jsem to zaplatil," svěřil se Jiří. Jenomže to neměl dělat. Krátce nato mu přišla další zpráva, v níž mu někdo oznamoval, že má jeho účet, a pokud ho chce zpátky, musí zaplatit výkupné. Jiří se stal obětí kybernetického útoku zvaného smishing.

Index Kybernetické bezpečnosti zpracovaný agenturou Ipsos pro Českou bankovní asociaci ukazuje, že hackerských útoků u nás přibývá a letos se s nim setkalo 27 procent Čechů.

Jedním z nejčastějších kybernetických útoků je právě smishing, se kterým se v poslední době potýká například i Česká pošta. „Útočník rozesílá podvodné SMS zprávy, které mají vzbudit dojem, že byly odeslány z České pošty. V případě, že si člověk není jistý, na zprávu doporučujeme nereagovat a kontaktovat infolinku České pošty," uvedl manažer specializovaného útvaru ICT České pošty Luděk Tichý.

PODEZŘELÉ ZPRÁVY RADĚJI NEOTVÍRAT

V případě České pošty útok nejčastěji probíhá tak, že příjemce dostane zprávu o nedoplatku za balík. Pod záminkou doplatku formou elektronické platby se útočník dostane k údajům o platební kartě a obratem obětí konto „vybílí". „V poslední době se objevuje i podvrh formou oznámení výplaty přeplatku na dani a snaha vymámit z oběti opět údaje k platební kartě a zaútočit na bankovní účet," upřesnil Tichý.

Rozpoznání podvodu ale není podle něho složité, protože Česká pošta platbu formou on-line karet neprovádí.

Etalonem hackerských technik je ale takzvaný phishing, který je populární pro svoji jednoduchost. Na rozdíl od smishingu útok probíhá prostřednictvím e-mailu, v němž se hacker rovněž vydává za banku, energetickou společnost nebo třeba i za kamaráda. Devadesát procent všech kybernetických útoků začíná právě phishingovým e-mailem.

„Útočníci v podvodných e-mailech chtějí, abyste udělali něco, co po vás nikdy žádná spolehlivá obchodní společnost či autorita prostřednictvím nevyžádaného e-mailu nebude požadovat: zadání údajů o platební kartě nebo hesel k internetovému bankovnictví, stáhnutí souboru zaslaného v příloze a podobně," přibližil bezpečnostní expert společnosti Cisco Milan Habrcetl.

Z bezpečnostní zprávy společnosti Cisco vyplývá, že phishing patří mezi čtyři nejčastější internetové hrozby. Stejná data pak ukazují, že phishingový útok obsahuje každý 99. e-mail. Třicet procent uživatelů pak takový e-mail otevře.

Jako užitečný návod, jak rozpoznat podvodné útoky, může posloužit Kybertest.cz, který připravila Česká bankovní asociace. V něm si každý může vyzkoušet svou zdatnost v kybernetické bezpečnosti.

Foto: ČTK

www.denik.cz/nazory

Dožijí se naše děti slušné penze? Premiér odpoví

KATEŘINA PERKNEROVÁ

Praha – Předlouhých šestadvacet let se v Česku řeší, jak nastavit důchodový systém. Jedna penzijní komise expertů střídala druhou, ale politická reprezentace se až do vlády Petra Nečase k ničemu neodhodlala. Teprve ta zavedla povinný druhý pilíř, který měl být vedle průběžného spořením další součástí konstrukce. Vydrželo to jen do doby, než se vlády ujali ČSSD s ANO a lidovci, kteří tuto novinku zrušili.

Současný ministr práce a sociálních věcí Marian Jurečka (KDU-ČSL) slibuje, že do konce příštího roku přijde s komplexní návrh, který odpoví na klíčové otázky. Například na to, proč je v ČR povinná doba pojištění skoro nejdelší v EU, tedy 35 let. Na důchod kvůli tomu nedosáhne sedm tisíc lidí ročně. Každý odpovědný kabinet musí řešit i skutečnost, že zatímco dnes činí podíl penzijních výdajů devět procent HDP, v roce 2060 to bude 14,5 procenta.

Všichni odborníci zdůrazňují, že je nutné zvýšit věkovou hranici odchodu do důchodu nad 65 let a zároveň jí provázat se změnou preventivního zdravotnictví, aby se prodloužil věk dožití ve zdraví. Kromě toho musí financování důchodového systému spoléhat na více zdrojů, především jde o třetí pilíř soukromého připojištění. Ekonom Miroslav Zámečník k tomu v ČT podotkl: „Dobře to opsat a nezprznit," čímž měl na mysli osvědčený švédský model. Je totiž neudržitelné, aby se nadále hradilo 77 procent důchodů z pojistného, když v EU je to 53 procent, jak připomíná ekonomka Danuše Nerudová.

Co na to říká premiér Petr Fiala? Uslyšíte v debatě dnes ve 12.00 na deník.cz

Astronauti na Marsu budou žít v jeskyních

KATEŘINA RAKÚSOVÁ

ZATÍM JEN SEN. I takto by podle vizualizace NASA mohla vypadat plánovaná lidská návštěva Marsu. Foto: NASA

Jedna věc je na Rudou planetu se dostat, druhou je, kde by na Marsu mohli astronauti bydlet. Odborníci přišli na to, že by jako obydlí mohly skvěle sloužit podzemní jeskyně podobné těm, jaké existují i na Zemi. A rovnou identifikovali devět míst, která by se k tomuto účelu perfektně hodila.

Vhodné jeskyně na Marsu naši vědci v oblasti Deuteronilus Mensae. Devět kandidátů pro ubytování astronautů prezentovali na setkání Geological Society of America Connects 2022 v Denveru. Deník New York Times píše, že všechny vytipované jeskyně sahají alespoň do určité hloubky pod zem a jsou blízko míst vhodných pro přistání lehkého vozítka.

Podzemní jeskyně mohou být bezpečnými příbytky, které případné obyvatele ochrání před drsnými podmínkami. „Vše na povrchu je vystaveno prudké radiaci, možnému bombardování meteority nebo mikrometeority a opravdu velkým teplotním výkyvům mezi dnem a nocí," řekla geoložka z Arizonské univerzity Nicole Bardabeliasová.

Problémem zatím je, že žádné z vozítek, které se na Rudé planetě nyní nachází, není dostatečně blízko, aby mohlo některou z vybraných jeskyní více prozkoumat. Tento úkol nyní připadá pouze kosmickým sondám na oběžné dráze planety.

Portál As doplňuje, že by jeskyně na Marsu mohl v budoucnu prozkoumávat robot Nebula-Spot, kterého sestavila NASA v projektu BRAILLE. Robot podobající se konstrukcí čtyřnohému zvířeti zatím zkoumá lávové jeskyně na Zemi. Připravuje se tak na příští mise v jeskyních na Marsu.

112. SMS nebo e-mail. Zprávy od hackerů umí nepozorné připravit o desetitisíce korun

Online ● denik.cz (Zprávy / Politika) ● 3. 11. 2022, 19:30

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)** ● Autor: **Vilém Janouš**

Dosah: 529 030 ● GRP: 5.88 ● OTS: 0.06 ● AVE: 58042.39 Kč ● Interakcí: 14

Odkaz: https://www.denik.cz/pocitace-a-mobily/hackerske-utoky-smishing-phishing.html

Chci zprávy do e-mailu

deník.cz

ZPRÁVY SPORT PODNIKÁNÍ NÁZORY MAGAZÍN PODCASTY MIMINKA O DENÍK

BYDLENÍ CESTUJEME AUTO VĚDA A TECHNIKA ŽENY ZDRAVÍ HOBBY | DOMÁCÍ VZDĚLÁVÁNÍ

PŘEHLEDNĚ: Předčasný důchod. Jak si měsíčně polepšit na penzi až o dva tisíce

SMS nebo e-mail. Zprávy od hackerů umí nepozorné připravit o desetitisíce korun

DNES 19:30

Vilém Janouš
Editor
Napište mi

Máte nedoplatek, který je potřeba ihned uhradit, oznámila jednačtyřicetiletému Jiřímu SMS. Tvářila se jako oficiální zpráva finančního úřadu a rovnou obsahovala odkaz na platbu. „Nechtěl jsem mít žádné problémy, tak jsem to zaplatil," svěřil se Jiří. Jenomže to neměl dělat. Krátce na tu mu přišla další zpráva, v níž mu někdo oznamoval, že má jeho účet a pokud ho chce zpátky, musí zaplatit výkupné. Jiří se stal obětí kybernetického útoku zvaného smishing.

Pozor na trojského koně. Triada dokáže pozměnit verifikační SMS zprávy, a manipulovat tak finančními transakcemi v legitimních aplikacích. | *Foto: Shutterstock*

Index Kybernetické bezpečnosti zpracovaný agenturou Ipsos pro Českou bankovní asociaci ukazuje, že hackerských útoků v České republice přibývá a letos se s ním setkalo dokonce 27 procent Čechů. Počet útoků se za poslední dva roky zvýšil čtyřnásobně, přičemž průměrná škoda dosahuje podle bankovní asociace 162 tisíc korun na jednoho klienta.

Jedním z nejčastějších kybernetických útoků je právě smishing, se kterým se v poslední době potýkají různé firmy, například Česká pošta. „Je to metoda podvodu, kdy útočník rozesílá podvodné SMS zprávy, které mají vzbudit dojem, že byly odeslány z České pošty. Ta doba, kdy zprávy bývaly psány špatnou češtinou s gramatickými a stylistickými chybami, je pryč. Dnes je podvrh více méně identický a je třeba zaměřit se na detail, například na odesílatele. V případě, že si člověk není jistý, na zprávu nereagovat a kontaktovat infolinku České pošty," uvedl manažer specializovaného útvaru ICT České pošty Luděk Tichý.

Hackeři masivně útočí na e-maily. Čechy se snaží nachytat na faktury z dovolené

PŘEČÍST ČLÁNEK ›

V případě České pošty útok nejčastěji probíhá tak, že příjemce dostane zprávu o nedoplatku za balík. Pod záminkou doplatku formou elektronické platby se útočník dostane k údajům o platební kartě a obratem oběti konto „vybílí“. „V poslední době se objevuje i podvrh formou oznámení výplaty přeplatku na dani a snaha vymámit z oběti údaje k platební kartě, a tak zaútočit na bankovní účet,“ upřesnil Tichý.

Rozpoznání podvodu ale podle něho není složité, protože Česká pošta platbu formou on-line karet neprovádí.

Bilionové škody

Základem hackerských technik je ale stále takzvaný phishing, který je populární pro svoji jednoduchost. Na rozdíl od smishingu útok probíhá prostřednictvím e-mailu, v němž se hacker rovněž vydává za banku, energetickou společnost nebo třeba i za kamaráda. Devadesát procent všech kybernetických útoků začíná právě phisingovým e-mailem.

„Útočníci v podvodných e-mailech chtějí, abyste udělali něco, co po vás nikdy žádná spolehlivá obchodní společnost či autorita prostřednictvím nevyžádaného e-mailu nebude požadovat: zadání údajů o platební kartě nebo hesel k internetovému bankovnictví, stáhnutí souboru zaslaného v příloze a podobně,“ přiblížil bezpečnostní expert společnosti Cisco Milan Habrcetl.

Nové vlny kyberzločinu cílí na mobily. Antiviry chrání jen 58 procent uživatelů

PŘEČÍST ČLÁNEK ›

Škody, které při těchto útocích vznikají, jsou obrovské. Americká FBI odhadla, že jen za rok 2021 dosáhly v přepočtu téměř bilion korun a útoků není ušetřena žádná země na světě. Jen mezi lety 2019 a 2021 jejich počet vzrostl o 65 procent.

Z bezpečnostní zprávy společnosti Cisco pak plyne, že phishing patří mezi čtyři nejčastější internetové hrozby. Ty další jsou těžba kryptoměn na napadeném počítači, škodlivé trojské koně nebo vyděračský software, takzvaný ransomware. Stejná data pak ukazují, že phishingový útok obsahuje každý 99. e-mail. Třicet procent uživatelů pak takový e-mail otevře.

Kontrolujte adresu i gramatiku

Je tedy jasné, jak se bránit. Takový e-mail neotvírat. Habrcetl doporučuje zkontrolovat jméno a e-mailovou adresu odesílatele, protože slova ve jméně nebo doména za „@" mohou být různě překroucená. Napovědět může i obsah a gramatika zprávy. Útočníci mohou použít překladač z cizího jazyka do češtiny.

Pozor na pochybné aplikace. Majitele mobilu v tichosti připraví o peníze

PŘEČÍST ČLÁNEK ›

Podezřelý je i časový nátlak a důležité je věnovat pozornost odkazům a přílohám. „Pokud máte pochybnosti, kontaktujte klientské centrum instituce, která vám e-mail poslala," doporučil expert.

Nový seriál Deníku: Digitální podvody. *Zdroj: Deník*

Jako užitečný návod, jak rozpoznat podvodné útoky, může posloužit i Kybertest.cz, který připravila Česká bankovní asociace. V něm si každý může vyzkoušet svou zdatnost v kybernetické bezpečnosti.

Odborníci ovšem upozorňují, že uživatelé by měli pamatovat i na ochranu svých zařízení. Měli by na nich mít nainstalovaný aktualizovaný antivirový program a spamový filtr. Rozhodně by lidé měli takto chránit i svůj mobilní telefon, protože mailová komunikace dnes často probíhá právě na nich.

113. Podvod s investicemi do kryptoměn

Online ● policie.cz (Jiné) ● 9. 11. 2022, 7:44

Dosah: 20 667 ● GRP: 0.23 ● OTS: 0.00 ● AVE: 19996.45 Kč

Odkaz: https://www.policie.cz/clanek/uzemni-utvary-sprava-severoceskeho-kraje-zpravodajstvi-podvod-s-investicemi-do-kryptomen.aspx

ZPRAVODAJSTVÍ

Úvodní strana / Útvary Policie ČR / Krajská

Policie České republiky – KŘP Ústeckého kraje

Podvod s investicemi do kryptoměn

LOUNSKO - Policisté prověřují další útok podvodníků.

Kryptoměny vstoupily do masového povědomí jako alternativa oficiální měny s vidinou rychlého zbohatnutí. Zájem o kryptoměnu se zvyšuje, i když její hodnota je proměnlivá. K tomu přispívá i snadná dostupnost různých kryptoměnových aplikací. Podvodníci si stále nachází nové způsoby, jak docílit vlastního obohacení, zejména když jde o anonymní platební nástroj. Bitcoin s rostoucí hodnotou přitahuje i stále více podvodníků. Ti zneužívají mnohdy nedostatečně informované uživatele, kteří v investici do kryptoměn vidí možnost rychlého zisku.

Internetové podvody bývají detailně promyšlené a mnohdy zahrnují též psychosociální aspekt – snahu o vyvolání důvěry, možnost získání významného profitu. Využívají například výhodné a časově omezené „nabídky". Poškozený nemusí zprvu tušit, že se stal obětí trestného činu. V některých případech to zjistí, až když se mu zablokuje počítač, dojde k neoprávněnému čerpání finančních prostředků z účtu a podobně.

V uplynulé době policisté na Podbořansku přijali oznámení týkající se podvodného jednání s investicemi do kryptoměny. Oznamovatelka byla kontaktována na sociální síti neznámou ženou pod záminkou transakcí spojených s kryptoměnou. Oznamovatelku přesvědčila, aby uskutečnila několik plateb, které měly být určeny pro zlepšení signálu těžby kryptoměny. Poškozená tak přišla o bezmála 134 tisíc korun. Dosud neznámý pachatel se dopustil trestného činu podvodu, přičemž mu při dopadení hrozí až pětiletý trest odnětí svobody.

Policie ČR varujeme občany před velkým množstvím výše popsaného protiprávního jednání. S touto problematikou se policisté potýkají každý den v rámci celého Ústeckého kraje. Proto dbejte zvýšené opatrnosti na cizí telefonáty, nikdy nikomu nedávejte přístupy k vašemu internetovému bankovnictví, neinstalujte si do svých počítačů program Anydesk – vzdálený přístup k počítači, nikomu neposílejte vaše ofocené doklady ani vaše osobní údaje s daty narození.

Vyzkoušej si **www.kybertest.cz** a zjisti, kde máš mezery. Buď připraven!

9. listopadu 2022
por. Mgr. Kamil Marek
Oddělení tisku a prevence
KŘP Ústeckého kraje

E-mailem Vytisknout

114. Index Kyberbezpečnosti 2022 se drží na vysoké úrovni. Pojišťovnám lidé věří

Online ● opojisteni.cz (Podnikání / Marketing / PR) ● 9. 11. 2022, 12:00

Vydavatel: **oPojištění. cz s.r.o. (cz-28400887)**

Dosah: 1 652 ● GRP: 0.02 ● OTS: 0.00 ● AVE: 5456.46 Kč

Odkaz: https://www.opojisteni.cz/technologie/kyberneticka-rizika/index-kyberbezpecnosti-2022-se-drzi-na-vysoke-urovni-pojistovnam-lide-veri/c:24031/

OPOJIŠTĚNÍ.CZ
Informace ze světa pojištění

Pojistný trh | Legislativa | Spektrum | Technologie | Zahraničí | Pracovní nabídky

InsurTech | Kybernetická rizika

Index Kyberbezpečnosti 2022 se drží na vysoké úrovni. Pojišťovnám lidé věří

9.11.2022 **Kybernetická rizika**, **Technologie**

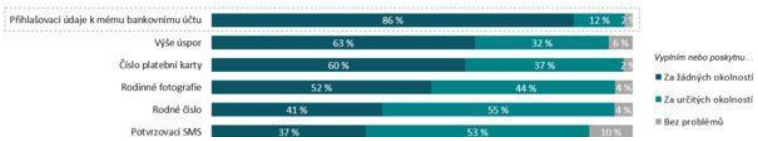
Češi jsou v online prostoru opatrní. Index Kyberbezpečnosti dosáhl 67 bodů a drží se tak blízko výsledku z loňského roku. Finanční operace lidé považují za citlivé a k internetovému či mobilnímu bankovnictví by nikdy neposkytla přístup většina z nich. Banky jsou pro Čechy nejdůvěryhodnější instituce, pokud jde o ochranu před únikem dat. Vyplývá to z průzkumu České bankovní asociace a výzkumné agentury Ipsos. Výsledkům průzkumu odpovídají i průběžná data Kybertestu, kterým během necelých dvou měsíců prošlo 54 tisíc lidí s průměrným výsledkem 70 %.

Index Kyberbezpečnosti dosáhl 67 bodů, o jeden bod méně než loni.

V loňském roce byly výsledky nejlepší od začátku sledování, index dosáhl 68 bodů. Letos je výsledek jen nepatrně nižší. Výsledky jsou z různých hledisek velmi vyrovnané. Lidé se základním vzděláním získali v průměru 65 bodů, zatímco vysokoškolsky vzdělaní získali průměrně 68 bodů. *„Zdá se, že lidé si uvědomují rizika, která jsou s online prostředím spojená. Naprostá většina by neposkytla přístupové údaje do internetového bankovnictví. Téměř dvě třetiny lidí kontrolují výdaje a úspory na účtu pravidelně,"* říká Petr Barák, expert České bankovní asociace na finanční a bankovní bezpečnost.

SDÍLENÍ OSOBNÍCH INFORMACÍ 1/2

Za žádných okolností by naprostá většina Čechů neposkytla přihlašovací údaje ke svému bankovnímu účtu a více než polovina pak výši úspor, číslo platební karty nebo rodinné fotografie. Ostatní informace jsou lidé ochotni sdílet za určitých okolností.

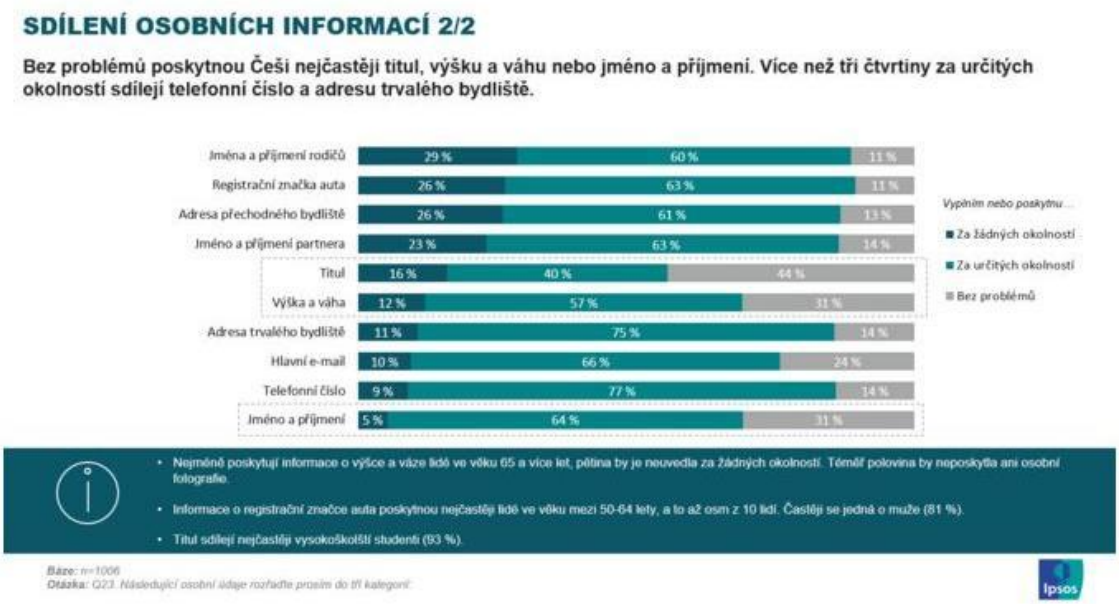


Češi jsou ve sdílení informací opatrní, čtvrtina ale někdy otevře neznámou přílohu

Za žádných okolností by přihlašovací údaje k účtu neposkytlo 86 % Čechů. Víc než polovina by nesdílela ani výši svých úspor, číslo platební karty nebo rodinné fotografie. Další informace jsou lidé ochotni sdělit pouze za určitých okolností. Více než tři čtvrtiny se v takových případech podělí o telefonní číslo a adresu trvalého bydliště. Téměř tři čtvrtiny lidí neotvírají přílohy od neznámých odesílatelů, čtvrtina však alespoň některou otevře. Upozornění banky na možné hrozby čte většina lidí a přibližně polovina to dokonce dělá pravidelně. Osm z deseti Čechů se do svého internetového bankovnictví připojuje přes vlastní zařízení, které je zcela pod jejich kontrolou.

„Česká populace je poměrně obezřetná v případě sdělování citlivých osobních údajů jako je číslo platební karty či přihlašovací údaje k bankovnímu účtu. Na druhou stranu však nemalá část lidí, přibližně čtvrtina, alespoň někdy otevírá přílohy emailů od neznámých uživatelů, což může způsobit vážný problém" uvádí Michal Straka z agentury Ipsos.

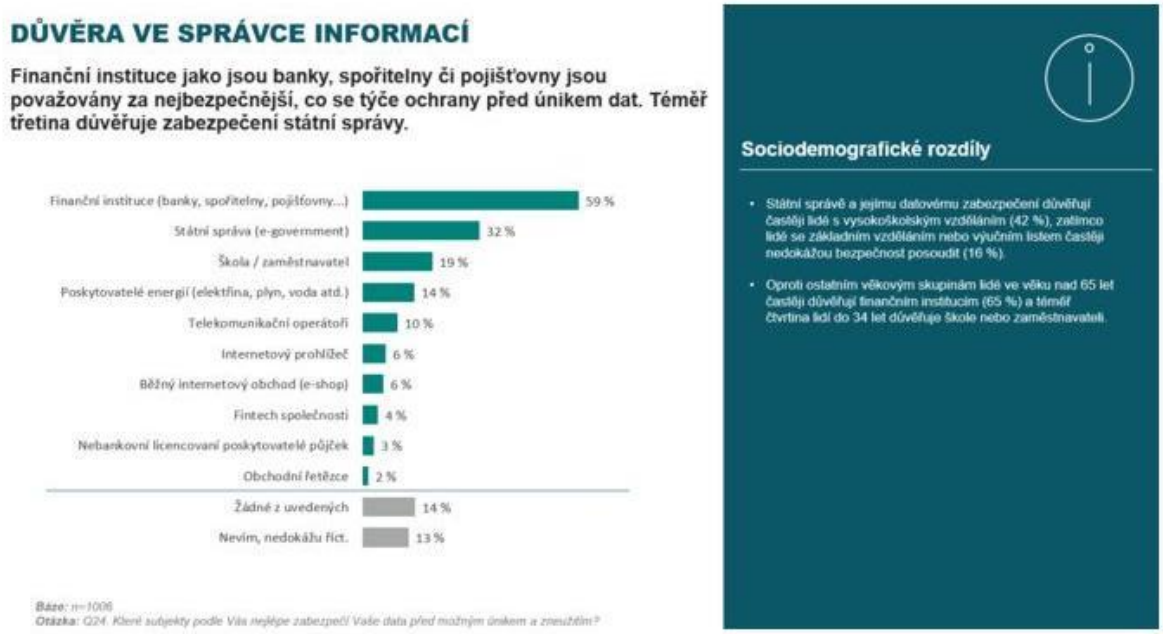
Mohlo by vás zajímat: Sestupný trend podnikatelských očekávání německých pojistitelů



Bankám a pojišťovnám věří lidé v ochraně údajů nejvíc

Banky, pojišťovny či spořitelny jsou považovány za nejbezpečnější, co se týče ochrany před únikem dat. Za důvěryhodné je považuje 59 % Čechů. Oproti tomu státní správu (e-government) vnímá bezpečně pouze necelá třetina. Nejnižší důvěru mají u lidí fintech společnosti, nebankovní poskytovatelé půjček a

obchodní řetězce.



Hackerských útoků přibývá, 27 % Čechů se s útokem setkalo letos

Víc než polovina Čechů se stala obětí hackerského útoku, a to bez ohledu na jeho dokončení. Třetina pak zná někoho, kdo byl obětí dokončeného útoku. Nejčastěji jde o podvodné e-maily, které slibují výhru v soutěži, popřípadě velké dědictví od zapomenutého člena rodiny. Víc než polovina má antivirový program v mobilním telefonu, u stolních počítačů je to sedm z deseti lidí. S útokem se nejčastěji setkávají lidé mezi 18 a 34 lety. 27 % Čechů se s útokem setkalo letos. Těmto údajům odpovídají i čísla České bankovní asociace. Počet útoků se za poslední dva roky zvýšil čtyřnásobně a průměrná škoda u dokončeného útoku je na jednoho klienta 162 tisíc korun. Útočníci nejčastěji cílí na získání přihlašovacích údajů, a to ve 40 % případů. Téměř třetina se pak snažila získat číslo platební karty a čtvrtina se zaměřila na osobní údaje, jako je například rodné číslo. Zájem byl také o heslo nebo PIN, a to ve 22 % případů.

Mohlo by vás zajímat: Pojišťovací Dr. Jekyll, nebo Mr. Hyde? Soud má jasno!

Do elektronického bankovnictví se lidé nejčastěji připojují přes Wi-Fi

Lidé se přes Wi-Fi připojují pouze v případech, kdy je dobře zabezpečená. Ve zvyku to má 44 % z nich. Více než čtvrtina lidí se pak připojuje kdekoli, a to pomocí datového tarifu. Na veřejných sítích své finance spravuje pouze 8 % Čechů. Šest z deseti lidí je běžně používají na vyřizování svých e-mailů a jiné korespondence. Téměř polovina (44 %) se pak tímto způsobem přihlašuje na sociální sítě.

„Připojovat se na veřejné, nezaheslované Wi-Fi není nikdy bezpečné. Nicméně lidé to dělají a budou dělat. Po připojení na veřejnou síť musí být lidé velmi ostražití a vstupovat do svého internetového či mobilního bankovnictví by vůbec neměli. Řada lidí si to ale stále neuvědomuje a kvůli tomu na sebe prozradí informace, které by prozrazovat neměli," říká Milan Habrcetl, Cyber Security Specialist společnosti Cisco.

Mohlo by vás zajímat: Jak přispělo zdražování firem ke dnešní inflaci v eurozóně?

Obchodování na on-line bazarech je časté, podvodné telefonáty lidé většinou odhalí

Téměř polovina Čechů někdy nakupovala na on-line bazarech a více než třetina na nich nějaké zboží prodávala. Nejčastější formou platby byl bankovní převod, ve čtyřech případech z deseti pak šlo o osobní předání. Podvodníci se často zaměřují právě na prodávající. Takových případů letos výrazně přibylo.

„Protože jsou prodávající klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům nebo do jejich internetového bankovnictví. Aby co nejdříve docílili prodeje zboží, neopatrně spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně. Opak je bohužel pravdou, většinou o všechno přijdou" objasnil pplk. Ondřej Kapr z Policie ČR. Pouze 3 % lidí by poskytla informace při falešném telefonátu. Víc než polovina z nich by pak situaci ověřila u banky.

Mohlo by vás zajímat: PwC: Češi si nechtějí říkat o více peněz. Zkusí to jen pětina zaměstnanců

Kybertest si vyzkoušely desítky tisíc lidí, úspěšnost je v průměru 70 %

Česká bankovní asociace ve spolupráci s partnery v září spustila celonárodní kampaň #nePINDej!, která má za cíl přivést lidi na stránky Kybertest.cz a tímto způsobem je vzdělávat. Za necelé dva měsíce od spuštění Kybertestu kampaň přilákala téměř 54 tisíc lidí, kteří testem prošli v průměru se 70% úspěšností. Kybertest se skládá z deseti nejčastějších podvodů a lidé si tak mohou vyzkoušet, jak odolní jsou proti případným hackerským útokům.

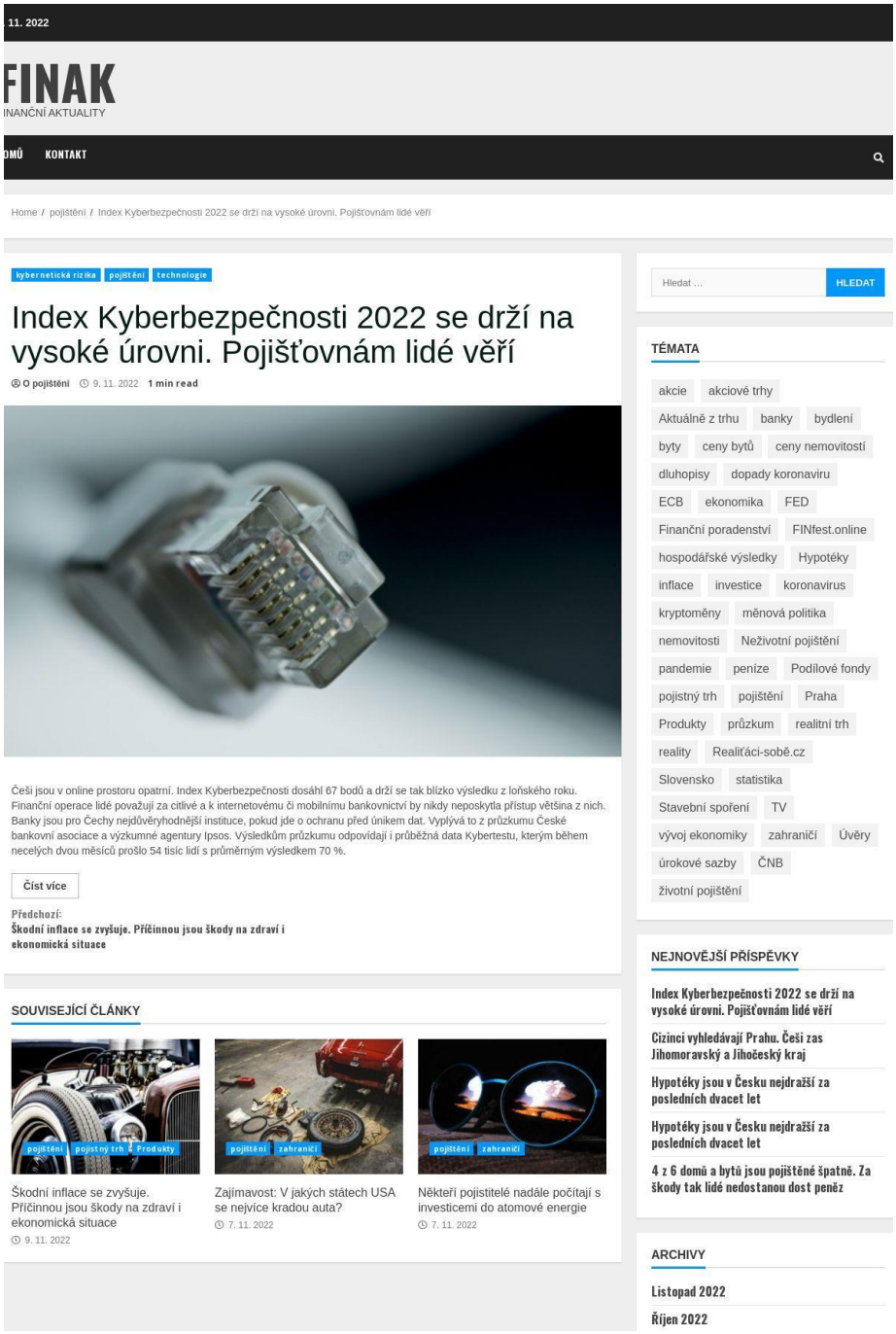
115. Index Kyberbezpečnosti 2022 se drží na vysoké úrovni. Pojišťovnám lidé věří

Online ● finak.cz (Ekonomika / Finance / Právo) ● 9. 11. 2022, 12:00

Rubrika: **kybernetická rizika**

Dosah: 34 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 688.56 Kč

Odkaz: https://www.finak.cz/index-kyberbezpecnosti-2022-se-drzi-na-vysoke-urovni-pojistovnam-lide-veri/



11. 2022

FINAK

INANČNÍ AKTUALITY

DOMŮ KONTAKT

Home / pojištění / Index Kyberbezpečnosti 2022 se drží na vysoké úrovni. Pojišťovnám lidé věří

kybernetická rizika pojištění technologie

Index Kyberbezpečnosti 2022 se drží na vysoké úrovni. Pojišťovnám lidé věří

O pojištění 9. 11. 2022 1 min read

Češi jsou v online prostoru opatrní. Index Kyberbezpečnosti dosáhl 67 bodů a drží se tak blízko výsledku z loňského roku. Finanční operace lidé považují za citlivé a k internetovému či mobilnímu bankovnictví by nikdy neposkytla přístup většina z nich. Banky jsou pro Čechy nejdůvěryhodnější instituce, pokud jde o ochranu před únikem dat. Vyplývá to z průzkumu České bankovní asociace a výzkumné agentury Ipsos. Výsledkům průzkumu odpovídají i průběžná data Kybertestu, kterým během necelých dvou měsíců prošlo 54 tisíc lidí s průměrným výsledkem 70 %.

Číst více

Předchozí:
Škodní inflace se zvyšuje. Příčinnou jsou škody na zdraví i ekonomická situace

SOUVISEJÍCÍ ČLÁNKY

pojištění pojistný trh Produkty
Škodní inflace se zvyšuje. Příčinnou jsou škody na zdraví i ekonomická situace
9. 11. 2022

pojištění zahraničí
Zajímavost: V jakých státech USA se nejvíce kradou auta?
7. 11. 2022

pojištění zahraničí
Někteří pojistitelé nadále počítají s investicemi do atomové energie
7. 11. 2022

Hledat … HLEDAT

TÉMATA

akcie akciové trhy Aktuálně z trhu banky bydlení byty ceny bytů ceny nemovitostí dluhopisy dopady koronaviru ECB ekonomika FED Finanční poradenství FINfest.online hospodářské výsledky Hypotéky inflace investice koronavirus kryptoměny měnová politika nemovitosti Neživotní pojištění pandemie peníze Podílové fondy pojistný trh pojištění Praha Produkty průzkum realitní trh reality Realiťáci-sobě.cz Slovensko statistika Stavební spoření TV vývoj ekonomiky zahraničí Úvěry úrokové sazby ČNB životní pojištění

NEJNOVĚJŠÍ PŘÍSPĚVKY

Index Kyberbezpečnosti 2022 se drží na vysoké úrovni. Pojišťovnám lidé věří
Cizinci vyhledávají Prahu. Češi zas Jihomoravský a Jihočeský kraj
Hypotéky jsou v Česku nejdražší za posledních dvacet let
Hypotéky jsou v Česku nejdražší za posledních dvacet let
4 z 6 domů a bytů jsou pojištěné špatně. Za škody tak lidé nedostanou dost peněz

ARCHIVY

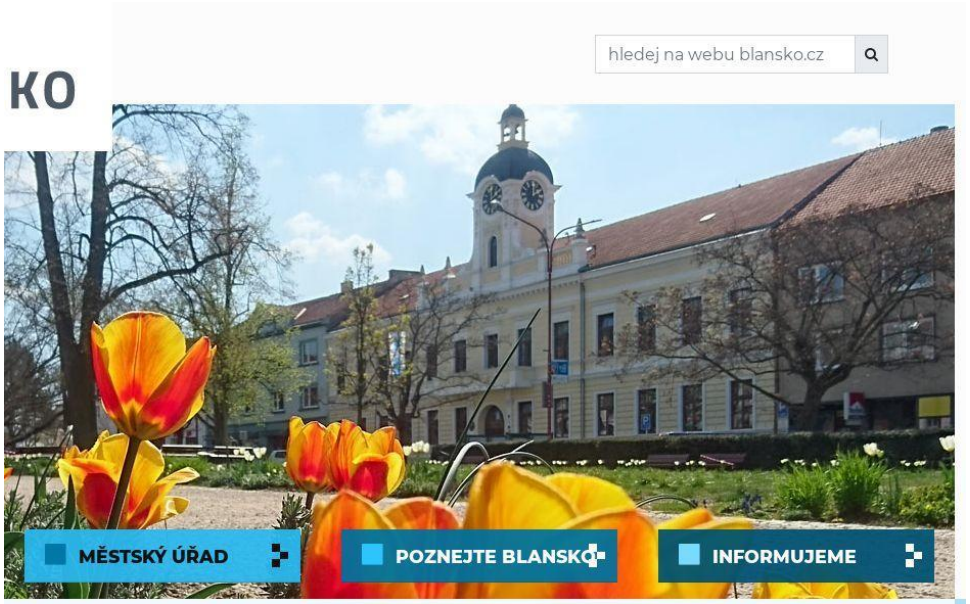
Listopad 2022
Říjen 2022

116. Články - Přibývá podvodů na klienty bank, policie a banky spustily vzdělávací kampaň #nePINdej!

Online ● blansko.cz (Regionální zprávy) ● 9. 11. 2022, 15:41

Dosah: 1 822 ● GRP: 0.02 ● OTS: 0.00 ● AVE: 7297.97 Kč

Odkaz: https://www.blansko.cz/clanky/2022/11/pribyva-podvodu-na-klienty-bank-policie-a-banky-spustily-vzdelavaci-kampan-nepindej



Články ▪ Článek

Přibývá podvodů na klienty bank, policie a banky spustily vzdělávací kampaň #nePINdej!

9. listopadu 2022, ostatní, přečteno: 16×

Policisté varují před podvodníky, kteří cílí na klienty bank. Počet takových útoků se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů. Police České republiky se připojila k rozsáhlé vzdělávací kampani #nePINdej! České bankovní asociace a dalších partnerů, která upozorňuje na sílící nebezpečí podvodů na internetu.

Obětí podvodníka se nedávno stal například šestačtyřicetiletý muž z Blanenska. Vše se odehrálo podle osvědčeného scénáře. Na začátku byl telefonát a oznámení, že při obchodování s kryptoměnou získal skoro čtyři tisíce dolarů, tedy skoro sto tisíc korun.

„Benefit bylo nutné převést na jeho účet. Muž tedy ochotně vyplnil emailem zaslaný podvodný formulář a poskytl potřebné údaje. Tím umožnil podvodníkovi především neomezený přístup k bankovnímu kontu. Z něj zmizelo více než sto tisíc korun. Navíc podvodník sjednal půlmiliónovou půjčku. Z možného zisku se tak vygenerovala velká ztráta," popsal případ policejní mluvčí Bohumil Malášek.

Podobně skončilo obchodování s kryptoměnou pro šestašedesátiletou ženu. I ona poskytla potřebné údaje. Dále zaplatila vstupní poplatek a nechala si nainstalovat program na vzdálenou správu počítače. „Pak už jen s odborníkem na kryptoměny sledovala, jak tento obchoduje. Výsledkem čtyřdenní činnosti byla ztráta více než třiceti tisíc korun. Potom podvodník komunikaci ukončil a žena pochopila, že se stala jeho obětí," doplnil policejní mluvčí.

Z dat České bankovní asociace vyplývá, že na jednoho poškozeného klienta připadá průměrná škoda ve výši 161 500 korun. U vishingu, neboli případů podvodného navolávání, jsou částky až čtvrtmilionové.

Klíčovým prvkem kampaně s názvem #nePINdej! (kreativní tvorba ze slov PIN nedej) je interaktivní vzdělávací www.kybertest.cz, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim předcházet.

„Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. Kybernetická kriminalita již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Kampaň proto cílí na širokou veřejnost počínaje dětmi a mladistvými přes dospělé až po seniory. Otázky v testu jsou tedy generovány dle věku uživatele," upřesnila policejní komisařka Lenka Koryťáková.

V kybertestu jsou simulovány podvodné SMS, zobrazovací okna k připojení k WIFI sítím, phishingové emaily, zvukové nahrávky podvodných telefonů a mnohé další, tak, aby si je každý uživatel moderních technologií mohl bezpečně vyzkoušet. Testové otázky byly připravovány odborníky na základě reálných případů, jimiž se podvodníci snaží své oběti nachytat.

Pachatelé se při těchto útocích snaží překonávat zejména lidský faktor a pod nejrůznějšími legendami využívají nátlaku, strachu a časové tísně pro záchranu peněz nebo pro realizaci finanční transakce.

Mezi nejčastější podvodné legendy patří:

1) Podvodné navolávání:

Pachatelé se vydávají například za bankéře, policisty, pracovníky technické podpory a snaží se z lidí pod vlivem strachu vylákat peníze, nebo vzdálený přístup do zařízení oběti, který následně zneužije.

2) Nabídka výhodných investic:

Přesvědčivá lákavá reklama a manipulativní jednání. Cílem pachatele je vylákat z oběti co možná nejvíce finančních prostředků a využívá k tomu přirozenou ziskuchtivost každého z nás.

3) Reverzní inzertní podvody:

Pachatel zareaguje na váš inzerát. Podstrčí vám fiktivní platební bránu, kde vyplníte citlivé bankovní údaje a místo peněz za inzerované zboží přicházíte o všechny úspory.

4) Podvody typu Nigerijské dopisy:

Princip, který funguje už více jak 100 let. Pachatelé sázejí na kvantitu. Vždy se najde někdo, kdo se nechá nachytat na slibovanou cennou zásilku nebo domnělou pomoc. Často zde hraje velkou roli láska.

5) Klasické podvody typu phishing a smishing:

Stále dokonalejší a složitě rozpoznatelné podvodné emaily a SMS nabídky. Na první pohled již nenajdeme podezřelé znaky.

„Stále častější praktikou jsou v současné době tzv. reverzní inzertní podvody. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou," upozornila Koryťáková.

Základní rady, jak nenaletět

- Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.
- Vyzkoušej si www.kybertest.cz a zjisti, kde máš mezery.

Zdroj: Policie ČR

117. Falešný bankéř dokáže ukrást miliony. Přes telefon

Tisk ● Slovácký deník; str. 6 (Regionální zprávy) ● 10. 11. 2022

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)**

Dosah: 542 613 ● GRP: 6.03 ● OTS: 0.06 ● AVE: 989352.97 Kč

Odkaz: náhled

UDÁLOSTI

Komentář

Luboš PALATA
redaktor

Dobrá zpráva z USA. Donald Trump nemá tak moc nabito

Měla to být republikánská tsunami, na které chtěl Donald Trump dosurfovat za dva roky do Bílého domu. Nepřesvědčivé vládnutí Joea Bidena tomu hodně nahrávalo. Biden nedokázal ani ve Spojených státech zabránit dopadům Ruskem způsobené globální energetické krize, a tím i slabšímu pocovidovému oživení ekonomiky. A na výkonu hlavy USA se začíná projevovat, že je prezidentovi už úctyhodných 79 let.

Prostě, v mezivolbách, které nyní proběhly ve Spojených státech, se čekalo, že voliči dají dvěma rokům Bidenova vládnutí trpké vysvědčení. A že to jinak než ovládnutím obou komor Kongresu republikány skončit ani nemůže. Ne, že by demokraté vyhráli, to se ostatně v Americe u prezidentské strany stává v těchto volbách jen zřídka. Ale ztratili méně, než bývá obvyklé. Nebylo to proto, že by Američané najednou byli s Bidenovým vládnutím spokojenější. Ale představa, že by se k zákonodárné moci dostala masa lidí z okruhu exprezidenta Donalda Trumpa, je prostě děsivá víc. A právě to, že kandidáti, které si Trump osobně vybral nebo je výrazně podporoval, nepatří často mezi vítěze těchto voleb, je pro Spojené státy ještě lepší zprávou. Zprávou o tom, že sice můžete být jako volič z Bidena zklamaní, ale pořád vám záleží na demokracii, kterou Trump svým zpochybňováním výsledků prezidentských voleb jasně ohrozil. A dodnes s tím nepřestal.

„Nejdůležitější zprávou voleb v USA není, že republikáni posílili. Ale to, že oslabil Donald Trump."

Vzhledem k Trumpovu chování a chování jeho mnohdy fanatických příznivců začíná být dnes vcelku jedno, kdo bude dalším americkým prezidentem. Důležité je jen to, aby to nebyl sám Trump. Nebo někdo z jeho následníků. Výsledek voleb do obou komor Kongresu a guvernérů by mohl části republikánů otevřít oči a pomoci vystoupit ze stínu Trumpa. Potřebovali by to jak republikáni, tak americká demokracie. Ta už musí přestat bojovat o život, ale potřebuje se co nejrychleji z Trumpa uzdravit.

Už zítra v Deníku

Kopeček: Kandidáti slibují nesplnitelné

Praha – Prezidentská volba se rozjíždí naplno. Tu přímou jsme zažili už dvakrát. Vždy zvítězil Miloš Zeman a politolog Lubomír Kopeček k němu v rozhovoru pro Deník řekl: „V politice toho hodně dokázal, ale nikdy neusiloval vytvořit nějaký trvalý ideový odkaz." Podle něj jsme se přímou volbou vmanévrovali do situace, kdy jsou prezidentští kandidáti vlastně nuceni nabízet věci, které prezident mnohdy splnit nemůže: „Typicky je to vidět na kampani Andreje Babiše a jeho slibech v oblasti ekonomiky, kde prezident nemá žádné pravomoci, jimiž by to mohl přímo ovlivňovat." A co si Lubomír Kopeček myslí o šancích jednotlivých kandidátů?

Dočtete se v zítřejším vydání Deníku. (kp)

Rozhovor s politologem Lubomírem Kopečkem čtěte již v pátek v Deníku

rozhovor Kateřiny Perknerové

Víte, že?

Deník pořádá už skoro deset let Kabelkový veletrh, jehož vítězek jen v jižních Čechách byl celkem 1,4 milionu korun.

Načtěte tento kód svým mobilním telefonem.

www.denik.cz/odeniku

Falešný bankéř dokáže ukrást miliony. Přes telefon

V Česku se množí případy takzvaného vishingu. Hackeři se při něm snaží přesvědčit své oběti, že jsou jejich peníze v ohrožení.

Digitální podvody
Jak bránit své peníze

VILÉM JANOUŠ

Irena z Poděbrad právě vyzvedávala děti ve školce, když ji zazvonil telefon. Na druhé straně se ozvala její údajná bankéřka s naléhavou zprávou, že ji na účtu probíhají podezřelé transakce. Řešením mělo být to, že Irena do telefonu nadiktuje přístupová data k internetovému bankovnictví. Samozřejmě to byl podvod a nešťastná žena se připravila o úspory. Stala se obětí takzvaného vishingu.

„Vishing, neboli podvodné navolávání, je jednou z nejúčinnějších technik, které online podvodníci využívají při získávání citlivých informací od obětí, nebo je jím vmanipulují do určitých situací. Cílem pachatelů je zejména finanční prospěch," přibližil Ondřej Kapr z policejního prezidia. Technika je založena na podvodných telefonátech a termín vychází z anglických slov voice a phishing. Jejím základem jsou manipulativní techniky sociálního inženýrství.

Předseda komise pro bankovní a finanční bezpečnost České bankovní asociace Petr Barák upozornil, že hackeři se na klienty bank začali výrazně zaměřovat předloni, kdy Evropa čelila koronavirové epidemii. Od loňska se pak množství phishingových útoků přetransformovalo do vishingu.

Odborník na kybernetickou bezpečnost společnosti BDO Martin Hořický považuje tuto techniku za nebezpečnou, protože útočník sází na neznalost nebo naivitu oběti. „Snaží se vás přesvědčit, že je zaměstnanec vaší banky, IT technik jiné pobočky vaší firmy či třeba nový nadřízený. Je velmi těžké identifikovat druhou stranu jenom na základě telefonního čísla," popsal Hořický.

Útočníci totiž dokážou změnit své telefonní číslo tak, že vypadá třeba jako číslo banky. „Lidé by si měli uvědomit, že nemohou vždy věřit informacím, kterou vidí na displeji," upozornil Kapr.

Hackeři v obětech vyvolávají časovou tíseň, například upozorněním na to, že jsou jejich peníze ohroženy. „V klientech vyvolávají obavu, že se skutečně něco děje s jejich účtem a ti pod tlakem začnou se záškodníky spolupracovat," přiblížil Barák.

Falešný bankéř poté navrhne postup, jak peníze zachránit. Například převést peníze na účet, který podvodníci vydávají za účet banky, nebo peníze vyzvednout a hotovost vložit třeba do bitcoinového bankomatu. V některých případech navrhnou převést peníze do investic, které neexistují, či přímo svou oběť k tomu, aby si nainstalovala do mobilu podvodnou aplikaci, která umožní vzdálený přístup. Přes ni pak zlodějům umožní přístup do svého internetového bankovnictví.

Ilustrační foto: Shutterstock

Policie se za poslední dva roky zabývala více než tisícovkou podobných případů. Česká bankovní asociace uvádí, že průměrná škoda je u těchto typů útoku asi čtvrt milionu korun. „Je potřeba, aby se lidé začali vzdělávat v kyberbezpečnosti a aby se zajímali o aktuální trendy. Když víte, co se právě děje, a jste na takovou situaci připravení, tak je pak daleko menší pravděpodobnost, že vás podvodník zaskočí," podotknul policista Kapr.

Jako užitečný návod, jak rozpoznat podvodné útoky, mohou posloužit webové stránky www.kybertest.cz, které připravila Česká bankovní asociace. Na nich si každý může vyzkoušet svou zdatnost v kybernetické bezpečnosti.

Procento dolů. Kde vláda najde sedmdesát miliard?

KATEŘINA PERKNEROVÁ

Praha – Česká ekonomika se nachází v mírné recesi. Podle aktuální makroekonomické predikce ministerstva financí skončí letošní veřejné finance ve schodku 4,6 procenta hrubého domácího produktu (HDP), což představuje nárůst zadlužení na téměř 44 procent HDP. Průměrná míra inflace by z letošních patnácti procent měla klesnout na 9,5 procenta. Vzhledem k letošnímu schodku 375 miliard a navrhovaným 295 miliardám na příští rok to žádný důvod k jásotu není.

Energetická krize tvrdě dopadá na domácnosti i firmy. Stát na kompenzace cen elektřiny a plynu musí vydávat desítky miliard. Jak ale včera řekl ministr financí Zbyněk Stanjura na setkání s novináři, díky kombinaci daně z neočekávaných zisků a zastropování tržních výrobních cen pro neplynové zdroje elektřiny by se tyto náklady a výdaje měly vynulovat. Nějak to ale neřeší strukturální schodek, který trvale činí 220 miliard korun.

A právě na ten cíli komplexní návrh Národní ekonomické rady vlády na příjmové i výdajové straně. Na dotaz Deníku Stanjura uvedl, že vláda o něm bude diskutovat, ale už nyní lze označit některé slepé uličky: „Jsou to sloučování obcí, rušení bonusu pět set korun k penzi za vychované dítě, zavedení školného nebo zvýšení daně z příjmu fyzických osob. Chceme ale příjmout opatření, jež strukturální schodek sníží o jedno procento HDP, což představuje zhruba 70 miliard korun." Cestu vidí v úpravě rozpočtového určení daní, úpravě rodičovské dovolené, penzijní reformě či rušení daňových výjimek.

Co na to říká premiér Petr Fiala? Uslyšíte v debatě dnes ve 12.00 na deník.cz.

Vědci přeložili první nápis psaný abecedou

MAGDALÉNA ŠKAPOVÁ

Zdroj: Prof. Insoll

Izraelští vědci přeložili vůbec první větu napsanou starověkou abecedou. Konkrétně jazykem Kanaánců, kteří v době bronzové žili v částech současného Izraele, Palestiny, Libanonu, Sýrie a Jordánska.

MEZNÍK V DĚJINÁCH

Tato věta se našla na malém hřebenu ze slonoviny (na snímku). Ten pochází zhruba z roku 1700 př. n. l. a zní asi takto: „Nechť tento kel vymýtí vši z vlasů i vousů!"

Tým, který podle britské Sky News hřeben v bývalém významném starověkém městě Lachiš v Izraeli našel, tvrdí, že jde o zaklínadlo, které má nepříjemné parazity odehnat.

„Je to první věta, která byla kdy v Izraeli nalezena v kanaánském jazyce," uvedl profesor Yosef Garfinkel z Hebrejské univerzity v Jeruzalémě a dodal: „Je to mezník v dějinách lidské schopnosti psát."

Profesor Garfinkel a jeho tým, jehož součástí jsou i kolegové z Jižní adventistické univerzity v USA, tvrdí, že hřeben pochází ze sloního klu. Má rozměry pouhých 3,5 × 2,5 centimetru a je zubatý na obou stranách. Samotné zuby jsou sice polámané, ale jejich základny jsou stále viditelné. Střední část je značně ohraněná – pravděpodobně kvůli tlaku prstů. Překvapivé je, že jeho design je podobný hřebenům s jemnými zuby, které se k vyčesávání vší a hnid používají i dnes.

Ačkoli byl vykopán již v roce 2017, rytina byla tak drobná, že si jí všimli až při následném zkoumání na začátku letošního roku. Následně ji rozluštil specialista na semitské jazyky Daniel Vainstub.

Nápis se skládá ze sedmnácti písmen a sedmi slov. „Je přímým důkazem používání abecedy v každodenních činnostech před přibližně 3 700 lety," vysvětlil Garfinkel.

více už brzy na denik.cz

118. Do škol letos s kybertestem. Připojit se může každý, kdo má chuť (a pracuje v bance)

Tisk ● Bankovnictví; str. 44, 45 (Ekonomika / Finance / Právo) ● 11. 11. 2022

Vydavatel: **4H production s.r.o. (cz-28471831)** ● Rubrika: **BANKY A FINANCE**

Dosah: 12 248 ● GRP: 0.14 ● OTS: 0.00 ● AVE: 158000.00 Kč

Odkaz: náhled

Do škol letos s kybertestem. Připojit se může každý, kdo má chuť (a pracuje v bance)

Od začátku října do konce listopadu se koná hlavní kolo přednášek na téma Finanční gramotnost a kyberbezpečnost na základních a středních školách po celé České republice v rámci již devátého ročníku projektu Bankéři do škol, který pořádá Česká bankovní asociace.

Finančně vzdělávací projekt Bankéři do škol iniciovala Česká bankovní asociace v r. 2014 a letos, jak již bylo řečeno, probíhá jeho už devátý ročník, který je speciální zejména v tom, že každá z přednášek pokrývá v menší či větší míře téma kybernetické bezpečnosti. To potvrzuje koneckonců také fakt, že v letošním roce byl do přednášek zařazen odkaz na interaktivní on-line kvíz – www.kyberhra.cz, který je obdobou oblíbeného kybertestu, ale obsahuje otázky vhodné pro žáky druhého stupně základních škol, středních škol a odborných učilišť a víceletých gymnázií.

Již přes 200 bankéřů

Projekt Bankéři do škol pořádá Česká bankovní asociace ve spolupráci se svými členskými bankami. V roli přednášejících jsou tedy bankovní specialisté z různých oblastí v bance, jejichž cílem je předat žákům a studentům zábavnou formou základní znalosti o financích a kybernetické bezpečnosti. Do letošního ročníku projektu se registrovalo více než 200 bankéřů (tedy zaměstnanců bank), kteří mají chuť a energii podělit se o své know-how s nadcházejícími generacemi.

Bankéři – přednášející – mají k dispozici prezentace, které obsahují všechny nejdůležitější informace k tématu s odkazy na související videa či vědomostní kvízy. „Nechováme však na přednášejících a jejich úsudku, jak budou přednášku vést. Hlavním záměrem je předat posluchačům zábavnou formou co největší množství informací," uvedla Andrea Machalová, koordinátorka projektu za Českou bankovní asociaci.

V kontextu výše zmíněného je třeba říct, že projekt Bankéři do škol se týká skutečně pouze zaměstnanců bank, nicméně, jak uvedl pro Bankovnictví Marek Černoch, výkonný ředitel České asociace společností finančního poradenství a zprostředkování (ČASF), také asociace uvažuje o působení v oblasti finančního vzdělávání. Další asociace EFPA potom spoluorganizuje každoročně Global Money Week, tudíž i externí finanční poradci se v oblasti finančního vzdělávání snaží angažovat.

GRAF 1 Rozřazení jednotlivých údajů podle ochoty sdílení

ZDROJ: ČBA

GRAF 2 Jakým institucím důvěřujete nejvíce?

ZDROJ: ČBA

Forma přednášek záleží na školách

Každoročně si potom školy mohou vybrat, zda svým žákům či studentům chtějí prostřednictvím přednášky, která trvá dvě vyučovací hodiny, přiblížit oblast finanční gramotnosti, či kyberbezpečnosti. „Během přednášky o finanční gramotnosti se posluchači seznámí se základními finančními pojmy. Dozvědí se například, co je to osobní účet, proč si mají vést osobní rozpočet, proč si mají spořit, kdy si vzít úvěry, jaká jsou úskalí zadlužování a jak funguje elektronické bankovnictví. Během přednášky o kyberbezpečnosti se seznámí s nejčastějšími typy kybernetických útoků, jak se jim bránit, jak se bezpečně pohybovat v on-line světě a jak zabezpečit své citlivé údaje," upřesnila Andrea Machalová.

V současné době je do letošního ročníku projektu Bankéři do škol přihlášeno bezmála 70 škol z různých koutů ČR. Projekt je koncipován pro žáky 8. a 9. tříd základních škol a studenty 1. a 2. ročníků středních škol a gymnázií.

Co se týče hodin, v jakých výuka probíhá, to záleží také převážně na škole a na tom, v rámci kterého školního předmětu přednášku uspořádá. Například v Rámcovém vzdělá-

Kyberbezpečnost je klíčové téma, i když jsou Češi v kyberprostoru opatrní

Jedním z klíčových témat České bankovní asociace je pro letošní rok bezesporu oblast kyberbezpečnosti, ke které mimo jiné také připravila kampaň #nePINdej!, o níž jsme psali v říjnovém Bankovnictví. Její součástí je právě výše zmíněný kybertest, který si už vyplnilo 54 tisíc lidí a jehož první výsledky ČBA představila ke konci října. Z nich vyplývá, že Češi jsou v on-line prostoru opatrní. Index kyberbezpečnosti dosáhl 67 bodů a drží se tak blízko výsledku z loňského roku (zde je ale třeba vzít v potaz fakt, že letošní test je propracovanější a náročnější).

Pozitivní je, že finanční operace lidé považují za citlivé a k internetovému či mobilnímu bankovnictví by nikdy většina z nich neposkytla přístup. Za žádných okolností by přihlašovací údaje k účtu neposkytlo 86 procent Čechů. Více než polovina by nesdílela ani výši svých úspor, číslo platební karty nebo rodinné fotografie. Další informace jsou lidé ochotni sdělit pouze za určitých okolností. Více než tři čtvrtiny se v takových případech podělí o telefonní číslo a adresu trvalého bydliště. Téměř tři čtvrtiny lidí neotvírají přílohy od neznámých odesílatelů, čtvrtina však alespoň některou otevře. Upozornění banky na možné hrozby čte většina lidí, a přibližně polovina to dokonce dělá pravidelně. Osm z deseti Čechů se do svého internetového bankovnictví připojuje přes vlastní zařízení, které je zcela pod jejich kontrolou.

„Česká populace je poměrně obezřetná v případě sdělování citlivých osobních údajů, jako je číslo platební karty či přihlašovací údaje k bankovnímu účtu. Na druhou stranu však nemalá část lidí, přibližně čtvrtina, alespoň někdy otevírá přílohy e-mailů od neznámých uživatelů, což může způsobit vážný problém," uvedl Michal Straka z agentury Ipsos.

Za bezpečné instituce jsou potom Čechy považovány banky, pojišťovny a spořitelny. Zejména co se týče oblasti úniku dat. Za důvěryhodné je považuje 59 procent Čechů. Oproti tomu státní správu (e-government) vnímá bezpečně pouze necelá třetina. Naopak nejnižší důvěru mají u lidí fintech společnosti, nebankovní poskytovatelé půjček a obchodní řetězce.

„Zdá se, že lidé si uvědomují rizika, která jsou s on-line prostředím spojená. Naprostá většina by neposkytla přístupové údaje do internetového bankovnictví. Téměř dvě třetiny lidí kontrolují výdaje a úspory na účtu pravidelně," dodal Petr Barák, expert České bankovní asociace na finanční a bankovní bezpečnost.

GRAF 3 Jaký typ hesla používáte k přístupu do:

ZDROJ: ČBA

vacím programu pro základní vzdělávání je finanční gramotnost začleněna do vzdělávacích oborů Člověk, stát a hospodářství a Člověk a jeho svět.

Témata nejsou pro žáky zcela neznámá

Standardy finanční gramotnosti jsou již několik let zařazeny do Rámcových vzdělávacích programů pro základní a střední školy. Proto většina témat souvisejících s finanční gramotností, která jsou součástí workshopů, není pro žáky a studenty úplnou novinkou. „Workshopy mají za cíl základní znalosti přehledně shrnout, na příkladech z praxe bankéřů či prostřednictvím kvízů a mediálních ukázek téma zatraktivnit a znalosti tak upevnit. Jistě se shodneme, že dostatek znalostí o financích a jejich správě je základem stabilní a bezpečné finanční budoucnosti. A my jsme rádi, že Bankéři do škol k tomu mohou svou měrou přispět," dodala Andrea Machalová s tím, že vzdělávací projekt Bankéři do škol umožňuje mimo jiné také pedagogům doplnit jinou formou předkládané učivo.

B | Text Redakce
www.bankovnictvionline.cz

> Workshopy mají za cíl základní znalosti přehledně shrnout, na příkladech z praxe bankéřů či prostřednictvím kvízů a mediálních ukázek téma zatraktivnit a znalosti tak upevnit.

119. Množí se telefonáty od falešných bankéřů. Lidé mohou přijít o statisíce

Online ● novojicinsky.denik.cz (Regionální zprávy) ● 11. 11. 2022, 4:00

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)** ● Autor: **Vilém Janouš**

Dosah: 1 494 253 ● GRP: 16.60 ● OTS: 0.17 ● AVE: 910271.32 Kč

Odkaz: https://novojicinsky.denik.cz/zpravy-z-ceska/vishing-telefonaty-od-falesnych-bankeru.html

Chci zprávy do e-mailu

NOVOJIČÍNSKÝ
deník.cz

ZPRÁVY SPORT PODNIKÁNÍ NÁZORY MAGAZÍN PODCASTY MIMINKA O DENÍK

PŘEHLEDNĚ: Předčasný důchod. Jak si měsíčně polepšit na penzi až o dva tisíce

Množí se telefonáty od falešných bankéřů. Lidé mohou přijít o statisíce

DNES 04:00

Vilém Janouš
Editor
Napište mi

Paní Irena z Poděbrad právě vyzvedávala děti ve školce, když jí zazvonil telefon. Na druhé straně se ozvala „její bankéřka“ s naléhavou zprávou, že na jejím účtu probíhají podezřelé transakce v zahraničí. Domnělá bankéřka vyděšené ženě vzápětí navrhla řešení, jak to zastavit: nadiktujte mi všechna přístupová data k internetovému bankovnictví. Paní Irena pak měla ještě po telefonu prozradit heslo a potvrdit odchozí platbu. Samozřejmě to byl podvod a nešťastná žena se tak připravila o nemalou finanční částku.

Vishing je založen na podvodných telefonátech, termín vychází z anglických slov voice a phishing. | *Foto: Shutterstock*

Stala se obětí takzvaného vishingu. „Vishing, neboli podvodné navolávání, je jednou z nejúčinnějších technik, které online podvodníci využívají při získávání citlivých informací od obětí, nebo touto technikou vmanipulují oběti do určitých situací. Cílem pachatelů je zejména finanční prospěch," přiblížil Ondřej Kapr z Policejního prezídia.

Tato technika je založena na podvodných telefonátech a termín vychází z anglických slov voice (hlas) a phishing (podvodná technika využívaná k získávání citlivých údajů). Jejím základem jsou manipulativní techniky sociálního inženýrství.

Pozor na falešné webové stránky bank. Podvodníci si mohou přijít na stovky tisíc

PŘEČÍST ČLÁNEK ›

Online útoky přitom nejsou nic nového a experti je zaznamenávají už někdy po

roce 2000. Předseda komise pro bankovní a finanční bezpečnost České bankovní asociace Petr Barák ale upozornil, že hackeři se na klienty bank začali výrazně zaměřovat předloni, kdy Evropa čelila koronavirové epidemii. Od loňska se pak množství phishingových útoků přetransformovalo do vishingu.

Partner a odborník na kybernetickou bezpečnost společnosti BDO považuje tuto techniku za poměrně nebezpečnou, protože sází na neznalost nebo naivitu člověka, na kterého cílí. „V tomto případě se vás může snažit přesvědčit, že je zaměstnanec vaší banky, IT technik jiné pobočky vaší firmy či například váš nový nadřízený. Z mého pohledu je velmi těžké identifikovat druhou stranu jenom na základě telefonního čísla," míní Hořický.

Nevěřit vlastnímu telefonu

Útočníci totiž dokáží zastřít nebo dokonce změnit svoje telefonní číslo na číslo banky nebo jiné instituce, za kterou se vydává. „Veřejnost by si měla uvědomit, že pachatel to dovede a že nemohou vždy věřit informaci, kterou vidí na displeji svého mobilního telefonu. Zobrazené telefonní číslo na displeji mobilního telefonu může být v některých případech doplněno i textem, který dále umocňuje přesvědčivost," upozornil Kapr.

Hackeři v takových případech vyvolávají časovou tíseň, když například falešný zástupce banky oznámí, že „vaše peníze jsou v ohrožení" nebo „přijali jsme žádost o půjčku", o které klient samozřejmě nic neví. „V klientech vyvolávají obavu, že se skutečně něco děje na jejich účtu a pod tímto ‚tlakem' pak s nimi klient začne spolupracovat," přiblížil Barák.

SMS nebo e-mail. Zprávy od hackerů umí nepozorné připravit o desetitisíce korun

PŘEČÍST ČLÁNEK ›

Falešný bankéř poté navrhne postup, jak peníze zachránit. Například převést peníze na účet, který podvodníci vydávají za účet banky, nebo peníze

peníze na účet, který podvodníci vydávají za účet banky, nebo peníze vyzvednout a hotovost vložit je třeba do bitcoinového bankomatu. V některých případech navrhnou převést peníze do investic, které neexistují, či přimějí svou oběť k tomu, aby si nainstalovalo do mobilního telefonu podvodnou aplikaci, která umožní vzdálený přístup. Přes ni pak zlodějům umožní přístup do svého internetového nebo mobilního bankovnictví.

Investice se zaručenou ztrátou

Zloději někdy mámí ze svých obětí peníze exkluzivní nabídkou do investic se zaručeným ziskem. „Telefonátu může předcházet vyplnění kontaktních údajů z vaší strany v rámci lákavých reklam na internetu, které jsou plné prvků sociálního inženýrství. Zejména jde o vyvolání dojmu snadného zisku a pocit exkluzivity," přiblížil Kapr.

Zdroj: Deník

Pachatelé se tak například snaží vylákat ze své oběti vzdálený přístup do počítače či mobilu. Přes tato zařízení pak může peníze ukrást. Jindy se snaží nalákat na výhodnou investici, která je ovšem pouze fikcí. Opět s cílem vylákat co nejvíce peněz.

„Tuto legendu mohou doprovázet fiktivní online investiční platformy s falešně rostoucími křivkami. Pachatelé se často zaštiťují renomovanými společnostmi a známými osobnostmi," doplnil policista.

Škoda za miliardu

Policie se za poslední dva roky zabývá více než tisícovkou případů a škody nejsou malé. Česká bankovní asociace uvádí, že průměrná škoda je u těchto typů útoku asi čtvrt milionu korun.

Bezpečnostní expert Barák tvrdí, že 99 procent všech útoků na klienty bank hackeři provádějí právě pomocí technik jako jsou vishing, phishing, smishig a podobně. Spočítal pak, že celková škoda, která v roce 2021 klientům bank těmito podvody vznikla, dosahuje jedné miliardy korun. „Dá se tedy očekávat, že s ohledem na letošní dvojnásobný nárůst počtu těchto případů se bohužel zdvojnásobí letos i celková škoda," doplnil Barák.

Falešné weby, bitcoiny či investice. Internetovým podvodníkům naletí i mladí

PŘEČÍST ČLÁNEK ›

Obezřetnost je tedy na místě. „Je potřeba, aby se lidé začali vzdělávat v kyberbezpečnosti a aby se zajímali o aktuální trendy. Když víte, co se právě děje a jste na takovou situaci připravení, tak je pak daleko menší pravděpodobnost, že vás podvodník zaskočí," míní policista Kapr.

Jako užitečný návod, jak rozpoznat podvodné útoky, může posloužit Kybertest.cz, který připravila Česká bankovní asociace. V něm si každý může vyzkoušet svou zdatnost v kybernetické bezpečnosti.

Podle Kapra totiž pachatelé zastihli veřejnost nepřipravenou. „Takový online podvodník se neustále vzdělává a každým pokusem se posouvá dál. Nakonec dokáže najít odpověď na jakoukoliv vaší otázku. Navíc si musíme uvědomit, že čím více informací o nás pachatel před útokem má, tím sofistikovanější útok na nás může připravit," dodal.

120. Berounští policisté řeší různé typy podvodných jednání. Troufalost pachatelů nezná mezí. Důvěřivost jejich obětí však také ne.

Online ● policie.cz (Jiné) ● 11. 11. 2022, 6:32

Dosah: 20 667 ● GRP: 0.23 ● OTS: 0.00 ● AVE: 19996.45 Kč

Odkaz: https://www.policie.cz/clanek/berounsti-policiste-resi-ruzne-typy-podvodnych-jednani-troufalost-pachatelu-nezna-mezi-duverivost-jejich-obeti-vsak-take-ne.aspx

ZPRAVODAJSTVÍ

Úvodní strana / Útvary Policie ČR / Krajská ředitelství policie / Středočes

Policie České republiky – KŘP Středočeského kraje

Berounští policisté řeší různé typy podvodných jednání. Troufalost pachatelů nezná mezí. Důvěřivost jejich obětí však také ne.

BEROUNSKO – Nechcete se stát obětí podvodu? Tak čtěte dále.

Berounští policisté téměř denně přijímají oznámení o podvodech spáchanými různými způsoby. Průběh spáchaných skutků je v drtivé většině totožný a chyby poškozených se stále dokola opakují. Připravili jsme pro vás rady jak nenaletět a nepřijít o peníze. Nejprve však popíšeme různé typy jednání, se kterými jsme se v praxi setkali.

Inzertní portály

Scénář těchto podvodů je jak přes „kopírák". Poškozená osoba prodává zboží na inzertních portálech. Přes mobilní aplikaci WhatsApp se jí ozve „kupující" se zájmem o zboží s tím, že zašle přes zprávu odkaz na přepravní společnost, která zprostředkuje přepravu zboží. Poškozená osoba na odkaz klikne a dostane se na webové stránky, které vypadají jako webové stránky různých přepravních společností (PPL CZ, Zásilkovna, DPD CZ s.r.o., Česká pošta, s. p.). Na těchto stránkách prodávající vyplní údaje ke svému bankovnímu účtu nebo k platební kartě, přístupové údaje a údaje k platební kartě. A co se stane? Poškozená osoba prostřednictvím jich „otevře" podvodníkovi dveře do svého internetového bankovnictví a k penězům, který jej začne ovládat, peníze převede na x dalších účtů, případně začne čerpat předschválenou půjčku či měnit limity na bankovním účtu.

Investice/zhodnocení peněz

Pojďme na scénář k tomuto typu podvodů a vezmeme příklad rovnou z praxe. Hořovičtí policisté přijali 29. září oznámení od ženy, kterou telefonicky kontaktoval neznámý muž s tím, že jí chce zaslat finanční hotovost, která jí zůstala na neidentifikovatelném účtu z dob obchodování s akciemi. Protože poškozená kdysi skutečně s akciemi obchodovala a domnívala se, že na dávném účtu jí nějaké finance mohly zbýt, tak se zasláním souhlasila. Do této doby je vše v pořádku. Ovšem následující postup by měl být pro ty, kteří nechtějí přijít o úspory, velkým varováním. Pachatel požadoval, aby si žena do notebooku nainstalovala aplikaci AnyDesk, což je aplikace umožňující dálkový přístup do počítače. Žena si aplikaci nainstalovala, poskytla pachateli kódy, díky kterým se přes zmíněnou aplikaci dostal do jejího počítače. Poté se v něm sám pohyboval. Po ženě chtěl naskenovat její občanský průkaz, požadoval údaje k její platební kartě včetně CVC kódu. Požadované poškozená pachateli poskytla. Po tomto ženě uvedl, že jí peníze začne zasílat postupně a je tak nutné, aby jejich přijetí odsouhlasila v internetovém bankovnictví. Poškozená se však neujistila, co potvrzuje a místo potvrzení přijetí peněz, potvrzovala v několika případech jejich odeslání. Tímto způsobem přišla o 100.000,-Kč. Berounští policisté se zabývají i oznámeními, kdy sami poškození reagovali na zveřejněné podvodné inzeráty nabízející zhodnocení peněz, popřípadě investování do kryptoměn. Podobným způsobem pak i oni přišli o své finance.

Falešné navolávání

V tomto případě jde o kontaktování poškozené osoby telefonicky, kdy se jí ozve podvodník, který se představí jako bankéř/policista s tím, že byl u ní zaznamenán pokus vzetí půjčky na její osobu. Poradí jí, že pro ochranu je nutné vyzvednout veškerou finanční hotovost z bankovního účtu a tu vložit na „bezpečný" účet. Poškozená osoba v domnění ochrany úspor vyzvedne finanční hotovost a tu vloží dle pokynů

„bankéře/policisty" do bitcoinmatu. V rámci tohoto skutečného oznámení, které jsme na Berounsku řešili, přišla poškozená žena o více než 350.000,-Kč. Podobně pachatelé útočí i pod legendou toho, že jsou bankéři/policisté, kteří zaznamenali z bankovních účtů poškozených podezřelé odchozí platby ve vysokých částkách. Pro „záchranu" peněz pak z poškozených dostanou veškerá přístupová hesla k jejich bankovním účtům. Ani v tomto případě se nejedná o dobrý skutek hodných lidí, ale o odčerpání maximální možné částky z bankovního účtu, a to za pomoci dobrovolně poskytnutých přístupových údajů.

Lékař/voják na misi

Tento způsob podvodů začíná nadějí na lepší život a nekonečnou láskou. Pokračuje půjčkami a končí prázdným kontem a očima pro pláč. Berounští policisté prověřovali případ ženy, kterou na sociální síti požádal o přátelství neznámý muž. Přátelství žena přijala, načež se muž představil jako americký voják toho času na misi v Afghanistánu. Po nějaké době konverzace se jí svěřil s tím, že by jí rád zaslal nějaké svoje dokumenty a hotovost, protože jen ona je pro něj důvěryhodnou osobou. Žena s přijetím balíku souhlasila. Postupně jí začal psát, že balíček drží celníci v Turecku, že byl zajat do vězení a potřebuje peníze na advokáta. Žena všemu věřila a postupně mu odeslala téměř 180.000,-Kč na celní poplatek a advokáta. Balíček, vojáka ani peníze už nikdy neuvidí.

Příspěvky na bydlení

Poškozeným osobám je doručena zpráva s nabídkou příspěvku na bydlení, popř. jiné sociální dávky. Osoba klikne na zaslaný odkaz ve zprávě, prostřednictvím kterého se dostane na webové stránky tvářící se jako stránky Ministerstva práce a sociálních věcí. Na těchto stránkách pak poškozená osoba vyplní požadavek v mobilní aplikaci internetového bankovnictví, který se tváří jako odsouhlasení přijetí sociálních dávek. Ovšem nepotvrzuje přijetí peněz, ale zaslání peněz pachateli. Berounští policisté prověřují oznámení poškozené ženy, která tímto způsobem přišla o 360.000,-Kč.

Nabídka dědictví

Dalším podvodem, který vyšetřují berounští policisté, je oznámení od muže, kterého kontaktovala osoba vydávající se za pracovníka kanadské banky. Ten oznamovateli sdělil, že se stal dědicem 20.000.000 USD a že je třeba zaplatit poplatek ze odmrazení účtu zemřelého a vyplacení dědictví. Poškozený postupoval dle pokynů „kanadského úředníka". Nejenže mu zaslal kopii svého občanského průkazu, ale pod vidinou dědictví uhradil také požadované poplatky. Jak už mnohé napovídá, tak se z oznamovatele nestal dědic, ale podvedený člověk s peněženkou lehčí o téměř 120.000,-Kč.

Jakkoliv se vám může popsané jednání zdát neuvěřitelné, tak je skutečné a vychází z případů, se kterými se berounští policisté setkávají téměř dnes a denně. V mnohých případech můžeme hovořit o naivitě poškozených, nicméně je třeba také zmínit, že některé typy podvodů jsou sofistikované a těžko rozeznatelné.

Chcete-li sami sebe otestovat a zjistit, zda jste schopní odolat podvodníků, doporučujeme vyzkoušet si **www.kybertest.cz**, který vznikl ve spolupráci Policie ČR s Českou bankovní asociací.

A jak podvodníků nenaletět?

- **Nikdy nikomu nesdělujte své přihlašující údaje do internetového bankovnictví ani čísla své platební karty. Banky ani policisté se na ně neptají, ani zprávami či e-mailem neposílají odkazy na weby, kde jsou vyžadovány.**
- **Nereagujte na hovory, e-maily ani zprávy, kde se vás někdo pokouší vmanipulovat do situace, že jsou vaše finanční prostředky v ohrožení a vy musíte udělat další kroky pro jejich záchranu. Kdyby byly vaše peníze v ohrožení, banka by zareagovala dávno bez vás.**
- **Pány účtu jste jen vy. Nezadávejte ani v aplikaci nepotvrzujte platby, které vám někdo bude diktovat po telefonu, ani nikomu nesdělujte či nepřeposílejte potvrzovací kódy z SMS. Stejně tak nedávejte nikomu vzdálený přístup do vašeho počítače.**
- **Mějte aktualizovaný software a antivirus, a to i na telefonu.**
- **V případě pochybností vždy kontaktujte svou banku či volejte 158. Myslete na to, že útočník dokáže napodobit jakékoliv telefonní číslo (spoofing) či e-mail, vč. těch vaší banky.**

nprap. Simona Vacherlohnová
preventistka P ČR ÚO Beroun
11. listopadu 2022

121. Policisté prověřují další útok podvodníků s investicemi do kryptoměn. Nachytat se nechala žena z Podbořanska

Online ● e-lounsko.cz (Regionální zprávy) ● 11. 11. 2022, 7:12

Vydavatel: **Oldřich Hájek (cz-74542338)** ● Autor: **re** ● Rubrika: **Zprávy**

Dosah: 683 ● GRP: 0.01 ● OTS: 0.00 ● AVE: 4384.17 Kč

Odkaz: http://www.e-lounsko.cz/zpravy/louny/213051-policiste-proveruji-dalsi-utok-podvodniku-s-investicemi-do-kryptomen-nachytat-se-nechala-zena-z-podboranska

proměniliva. K tomu přispívá i snadná dostupnost různých kryptoměnových aplikací. Podvodníci si stále nachází nové způsoby, jak docílit vlastního obohacení, zejména když jde o anonymní platební nástroj.

Internetové podvody bývají detailně promyšlené a mnohdy zahrnují též psychosociální aspekt – snahu o vyvolání důvěry, možnost získání významného profitu. Využívají například výhodné a časově omezené „nabídky". Poškozený nemusí zprvu tušit, že se stal obětí trestného činu. V některých případech to zjistí, až když se mu zablokuje počítač, dojde k neoprávněnému čerpání finančních prostředků z účtu a podobně.

"V uplynulé době policisté na Podbořansku přijali oznámení týkající se podvodného jednání s investicemi do kryptoměny. Oznamovatelka byla kontaktována na sociální síti neznámou ženou pod záminkou transakcí spojených s kryptoměnou. Oznamovatelku přesvědčila, aby uskutečnila několik plateb, které měly být určeny pro zlepšení signálu těžby kryptoměny. Poškozená tak přišla o bezmála 134 tisíc korun. Dosud neznámý pachatel se dopustil trestného činu podvodu, přičemž mu při dopadení hrozí až pětiletý trest odnětí svobody," uvedl k případu policejní mluvčí Kamil Marek.

Policie ČR varujeme občany před velkým množstvím výše popsaného protiprávního jednání. S touto problematikou se policisté potýkají každý den v rámci celého Ústeckého kraje. Proto dbejte zvýšené opatrnosti na cizí telefonáty, nikdy nikomu nedávejte přístupy k vašemu internetovému bankovnictví, neinstalujte si do svých počítačů program Anydesk – vzdálený přístup k počítači, nikomu neposílejte vaše ofocené doklady ani vaše osobní údaje s daty narození.

Vyzkoušejte si www.kybertest.cz a zjistěte, kde máte mezery.

122. Policisté prověřují další útok podvodníků s investicemi do kryptoměn. Nachytat se nechala žena z Podbořanska

Online ● e-zatecko.cz (Regionální zprávy) ● 11. 11. 2022, 8:09

Autor: **Jitka Fárová** ● Rubrika: **Zprávy**

Dosah: 686 ● GRP: 0.01 ● OTS: 0.00 ● AVE: 4392.91 Kč

Odkaz: https://e-zatecko.cz/zpravy/3969-policiste-proveruji-dalsi-utok-podvodniku-s-investicemi-do-kryptomen-nachytat-se-nechala-zena-z-podboranska

e-zatecko

Hledat...

Přihlásit se

DNES VYŠLO | ZPRAVODAJSTVÍ | CO SE CHYSTÁ | ZAJÍMAVOSTI | TIPY NA VÝLET | REGIO

e-Žatecko.cz › Zpravodajství › Policisté prověřují další útok podvodníků s investicemi do kryptoměn. Nachytat se nechala žena z Podbořanska

Policisté prověřují další útok podvodníků s investicemi do kryptoměn. Nachytat se nechala žena z Podbořanska

Autor článku Jitka Fárová

11.11.2022 08:09 | 10 zhlédnutí | Napište první komentář

Lounsko - Kryptoměny vstoupily do masového povědomí jako alternativa oficiální měny s vidinou rychlého zbohatnutí. Zájem o kryptoměnu se zvyšuje, i když její hodnota je proměnlivá. K tomu přispívá i snadná dostupnost různých kryptoměnových aplikací. Podvodníci si stále nachází nové způsoby, jak docílit vlastního obohacení, zejména když jde o anonymní platební nástroj.

Internetové podvody bývají detailně promyšlené a mnohdy zahrnují též psychosociální aspekt – snahu o vyvolání důvěry, možnost získání významného profitu. Využívají například výhodné a časově omezené „nabídky". Poškozený nemusí zprvu tušit, že se stal obětí trestného činu. V některých případech to zjistí, až když se mu zablokuje počítač, dojde k neoprávněnému čerpání finančních prostředků z účtu a podobně.

"V uplynulé době policisté na Podbořansku přijali oznámení týkající se podvodného jednání s investicemi do kryptoměny. Oznamovatelka byla kontaktována na sociální síti neznámou ženou pod záminkou transakcí spojených s kryptoměnou. Oznamovatelku přesvědčila, aby uskutečnila několik plateb, které měly být určeny pro zlepšení signálu těžby kryptoměny. Poškozená tak přišla o bezmála 134 tisíc korun. Dosud neznámý pachatel se dopustil trestného činu podvodu, přičemž mu při dopadení hrozí až pětiletý trest odnětí svobody," uvedl k případu policejní mluvčí Kamil Marek.

Policie ČR varujeme občany před velkým množstvím výše popsaného protiprávního jednání. S touto problematikou se policisté potýkají každý den v rámci celého Ústeckého kraje. Proto dbejte zvýšené opatrnosti na cizí telefonáty, nikdy nikomu nedávejte přístupy k vašemu internetovému bankovnictví, neinstalujte si do svých počítačů program Anydesk – vzdálený přístup k počítači, nikomu neposílejte vaše ofocené doklady ani vaše osobní údaje s daty narození.

Vyzkoušejte si www.kybertest.cz a zjistěte, kde máte mezery.

Čtěte také

Poznejte místo v Ústeckém kraji: Víte, kde stojí tajemný menhir připomínající shrbenou stařenu?

Vydejte se na Energy tour! Na vlastní oči se můžete podívat do velké uhelné elektrárny

TIP NA VÍKEND: Z České Lípy vyrazí parní lokomotivy

TIP NA VÝLET: Máte rádi chilli papričky? Tyto exotické pálivé krásky si teď můžete přijít prohlédnout zblízka

OBRAZEM: Děsí vás trochu toto tajemné místo? Krušnohorská osada byla vymazána z map

Reklama

REKULTIVUJEM

JSME NA FACEBOOKU

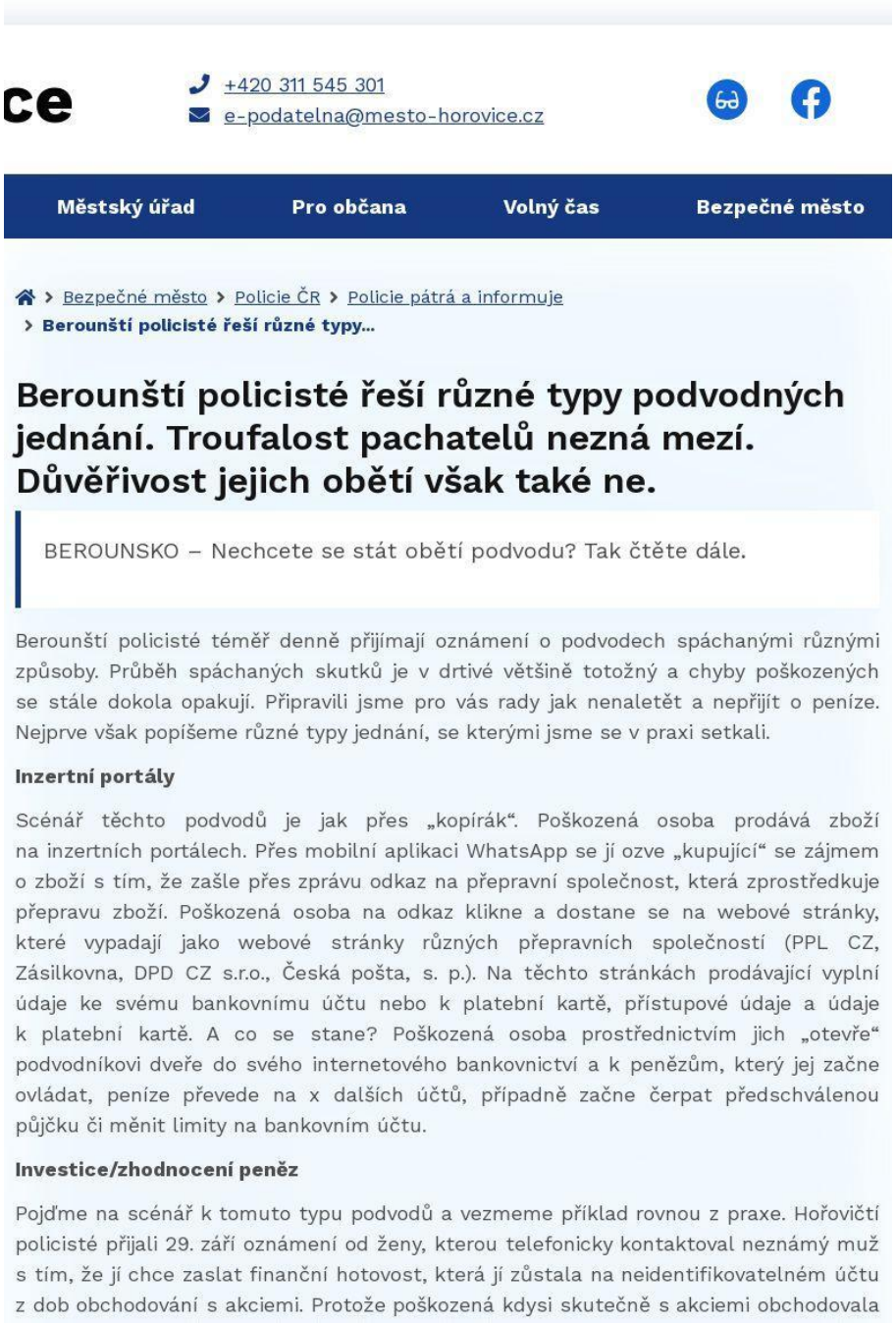
123. Berounští policisté řeší různé typy podvodných jednání. Troufalost pachatelů nezná mezí. Důvěřivost jejich obětí však také ne.

Online ● mesto-horovice.eu (Regionální zprávy) ● 11. 11. 2022, 8:22

Autor: **Simona Vacherlohnová**

Dosah: 215 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 2223.99 Kč

Odkaz: https://www.mesto-horovice.eu/bezpecne-mesto-1/policie-cr/policie-patra-a-informuje-1/berounsti-policiste-resi-ruzne-typy-podvodnych-jednani-troufalost-pachatelu-nezna-mezi-duverivost-jejich-obeti-vsak-take-ne-1516cs.html



ce

+420 311 545 301
e-podatelna@mesto-horovice.cz

Městský úřad | Pro občana | Volný čas | Bezpečné město

Bezpečné město › Policie ČR › Policie pátrá a informuje
› Berounští policisté řeší různé typy...

Berounští policisté řeší různé typy podvodných jednání. Troufalost pachatelů nezná mezí. Důvěřivost jejich obětí však také ne.

> BEROUNSKO – Nechcete se stát obětí podvodu? Tak čtěte dále.

Berounští policisté téměř denně přijímají oznámení o podvodech spáchanými různými způsoby. Průběh spáchaných skutků je v drtivé většině totožný a chyby poškozených se stále dokola opakují. Připravili jsme pro vás rady jak nenaletět a nepřijít o peníze. Nejprve však popíšeme různé typy jednání, se kterými jsme se v praxi setkali.

Inzertní portály

Scénář těchto podvodů je jak přes „kopírák“. Poškozená osoba prodává zboží na inzertních portálech. Přes mobilní aplikaci WhatsApp se jí ozve „kupující“ se zájmem o zboží s tím, že zašle přes zprávu odkaz na přepravní společnost, která zprostředkuje přepravu zboží. Poškozená osoba na odkaz klikne a dostane se na webové stránky, které vypadají jako webové stránky různých přepravních společností (PPL CZ, Zásilkovna, DPD CZ s.r.o., Česká pošta, s. p.). Na těchto stránkách prodávající vyplní údaje ke svému bankovnímu účtu nebo k platební kartě, přístupové údaje a údaje k platební kartě. A co se stane? Poškozená osoba prostřednictvím jich „otevře“ podvodníkovi dveře do svého internetového bankovnictví a k penězům, který jej začne ovládat, peníze převede na x dalších účtů, případně začne čerpat předschválenou půjčku či měnit limity na bankovním účtu.

Investice/zhodnocení peněz

Pojďme na scénář k tomuto typu podvodů a vezmeme příklad rovnou z praxe. Hořovičtí policisté přijali 29. září oznámení od ženy, kterou telefonicky kontaktoval neznámý muž s tím, že jí chce zaslat finanční hotovost, která jí zůstala na neidentifikovatelném účtu z dob obchodování s akciemi. Protože poškozená kdysi skutečně s akciemi obchodovala

a domnívala se, že na dávném účtu jí nějaké finance mohly zbýt, tak se zasláním souhlasila. Do této doby je vše v pořádku. Ovšem následující postup by měl být pro ty, kteří nechtějí přijít o úspory, velkým varováním. Pachatel požadoval, aby si žena do notebooku nainstalovala aplikaci AnyDesk, což je aplikace umožňující dálkový přístup do počítače. Žena si aplikaci nainstalovala, poskytla pachateli kódy, díky kterým se přes zmíněnou aplikaci dostal do jejího počítače. Poté se v něm sám pohyboval. Po ženě chtěl naskenovat její občanský průkaz, požadoval údaje k její platební kartě včetně CVC kódu. Požadované poškozená pachateli poskytla. Po tomto ženě uvedl, že jí peníze začne zasílat postupně a je tak nutné, aby jejich přijetí odsouhlasila v internetovém bankovnictví. Poškozená se však neujistila, co potvrzuje a místo potvrzení přijetí peněz, potvrzovala v několika případech jejich odeslání. Tímto způsobem přišla o 100.000,-Kč. Berounští policisté se zabývají i oznámeními, kdy sami poškození reagovali na zveřejněné podvodné inzeráty nabízející zhodnocení peněz, popřípadě investování do kryptoměn. Podobným způsobem pak i oni přišli o své finance.

Falešné navolávání

V tomto případě jde o kontaktování poškozené osoby telefonicky, kdy se jí ozve podvodník, který se představí jako bankéř/policista s tím, že byl u ní zaznamenán pokus vzetí půjčky na její osobu. Poradí jí, že pro ochranu je nutné vyzvednout veškerou finanční hotovost z bankovního účtu a tu vložit na „bezpečný“ účet. Poškozená osoba v domnění ochrany úspor vyzvedne finanční hotovost a tu vloží dle pokynů „bankéře/policisty“ do bitcoinmatu. V rámci tohoto skutečného oznámení, které jsme na Berounsku řešili, přišla poškozená žena o více než 350.000,-Kč. Podobně pachatelé útočí i pod legendou toho, že jsou bankéři/policisté, kteří zaznamenali z bankovních účtů poškozených podezřelé odchozí platby ve vysokých částkách. Pro „záchranu“ peněz pak z poškozených dostanou veškerá přístupová hesla k jejich bankovním účtům. Ani v tomto případě se nejedná o dobrý skutek hodných lidí, ale o odčerpání maximální možné částky z bankovního účtu, a to za pomoci dobrovolně poskytnutých přístupových údajů.

Lékař/voják na misi

Tento způsob podvodů začíná nadějí na lepší život a nekonečnou láskou. Pokračuje půjčkami a končí prázdným kontem a očima pro pláč. Berounští policisté prověřovali případ ženy, kterou na sociální síti požádal o přátelství neznámý muž. Přátelství žena přijala, načež se muž představil jako americký voják toho času na misi v Afghanistánu. Po nějaké době konverzace se jí svěřil s tím, že by jí rád zaslal nějaké svoje dokumenty a hotovost, protože jen ona je pro něj důvěryhodnou osobou. Žena s přijetím balíku souhlasila. Postupně jí začal psát, že balíček drží celníci v Turecku, že byl zajat do vězení a potřebuje peníze na advokáta. Žena všemu věřila a postupně mu odeslala téměř 180.000,-Kč na celní poplatek a advokáta. Balíček, vojáka ani peníze už nikdy neuvidí.

Příspěvky na bydlení

Poškozeným osobám je doručena zpráva s nabídkou příspěvku na bydlení, popř. jiné

sociální dávky. Osoba klikne na zaslaný odkaz ve zprávě, prostřednictvím kterého se dostane na webové stránky tvářící se jako stránky Ministerstva práce a sociálních věcí. Na těchto stránkách pak poškozená osoba vyplní požadavek v mobilní aplikaci internetového bankovnictví, který se tváří jako odsouhlasení přijetí sociálních dávek. Ovšem nepotvrzuje přijetí peněz, ale zaslání peněz pachateli. Berounští policisté prověřují oznámení poškozené ženy, která tímto způsobem přišla o 360.000,-Kč.

Nabídka dědictví

Dalším podvodem, který vyšetřují berounští policisté, je oznámení od muže, kterého kontaktovala osoba vydávající se za pracovníka kanadské banky. Ten oznamovateli sdělil, že se stal dědicem 20.000.000 USD a že je třeba zaplatit poplatek ze odmrazení účtu zemřelého a vyplacení dědictví. Poškozený postupoval dle pokynů „kanadského úředníka“. Nejenže mu zaslal kopii svého občanského průkazu, ale pod vidinou dědictví uhradil také požadované poplatky. Jak už mnohé napovídá, tak se z oznamovatele nestal dědic, ale podvedený člověk s peněženkou lehčí o téměř 120.000,-Kč.

Jakkoliv se vám může popsané jednání zdát neuvěřitelné, tak je skutečné a vychází z případů, se kterými se berounští policisté setkávají téměř dnes a denně. V mnohých případech můžeme hovořit o naivitě poškozených, nicméně je třeba také zmínit, že některé typy podvodů jsou sofistikované a těžko rozeznatelné.

Chcete-li sami sebe otestovat a zjistit, zda jste schopní odolat podvodníků, doporučujeme vyzkoušet si www.kybertest.cz, který vznikl ve spolupráci Policie ČR s Českou bankovní asociací.

A jak podvodníků nenaletět?

- **Nikdy nikomu nesdělujte své přihlašující údaje do internetového bankovnictví ani čísla své platební karty. Banky ani policisté se na ně neptají, ani zprávami či e-mailem neposílají odkazy na weby, kde jsou vyžadovány.**

- **Nereagujte na hovory, e-maily ani zprávy, kde se vás někdo pokouší vmanipulovat do situace, že jsou vaše finanční prostředky v ohrožení a vy musíte udělat další kroky pro jejich záchranu. Kdyby byly vaše peníze v ohrožení, banka by zareagovala dávno bez vás.**

- **Pány účtu jste jen vy. Nezadávejte ani v aplikaci nepotvrzujte platby, které vám někdo bude diktovat po telefonu, ani nikomu nesdělujte či nepřeposílejte potvrzovací kódy z SMS. Stejně tak nedávejte nikomu vzdálený přístup do vašeho počítače.**

- **Mějte aktualizovaný software a antivirus, a to i na telefonu.**

- **V případě pochybností vždy kontaktujte svou banku či volejte 158. Myslete na to, že útočník dokáže napodobit jakékoliv telefonní číslo (spoofing) či e-mail, vč. těch vaší banky.**

124. Zloději líčí pasti. Touží po platebních kartách

Tisk ● Tachovský deník; str. 6 (Regionální zprávy) ● 16. 11. 2022

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)**

Dosah: 542 613 ● GRP: 6.03 ● OTS: 0.06 ● AVE: 991529.40 Kč

Odkaz: náhled

6 Deník www.denik.cz 16. listopadu 2022

UDÁLOSTI

24 hodin na Ukrajině

Bombardovaná města zdobí Banksyho graffiti

Kyjev – Britský umělec Banksy potvrdil serveru The Art Newspaper, že na Ukrajině vytvořil sedm graffiti, a to v Kyjevě a také v Irpini a Borodance, které nejvíce utrpěly ruským bombardováním v jarní fázi války. Přihlásil se třeba k nástěnné malbě ukrajinské gymnastky na budově poničené ruským ostřelováním. Snímek graffiti v městečku Borodanka, které leží asi 50 kilometrů severozápadně od Kyjeva, zveřejnil autor na svém Instagramu. Gymnastka cvičí uprostřed trosek, napsala britská stanice BBC. Text i foto: ČTK

CO SE TAKÉ VČERA STALO

MUČENÍ. Rusko i Ukrajina mučily válečné zajatce, včetně šoků elektrickým proudem a nuceného svlékání. Uvedla to šéfka mise OSN monitorující humanitární situaci Matilda Bognerová. Prohlášení je založeno na svědectví 159 mužů a žen zajatých Ruskem a 175 mužů zajatých ukrajinskou stranou. **KONTROLA ČERNOBYLU.** Mezinárodní agentura pro atomovou energii se chystá v nadcházejících týdnech na ukrajinskou žádost vyslat kontrolní mise do Černobylské jaderné elektrárny a do dalších tří funkčních ukrajinských jaderných zařízení.

NAJDETE NA WWW.DENIK.CZ

MILIONY LIDÍ BEZ PROUDU. Rusko včera při nové vlně vzdušných útoků, podle Kyjeva nejrozsáhlejších od začátku války, vypálilo střely na města a energetickou infrastrukturu po celé Ukrajině. Energetická situace je kritická, uvedl zástupce šéfa ukrajinské prezidentské kanceláře Kyrylo Tymošenko. Přes sedm milionů domácností bylo bez proudu. V Kyjevě si útoky vyžádaly nejméně jednu oběť.

Dění na Ukrajině sledujeme online

Krátce

Dluhy má více než polovina obcí. Roste zadlužení krajů

OBECNÍ ROZPOČTY. Dluhy obcí se loni meziročně snížily o 1,5 miliardy korun na 69,6 miliardy. Přesto dluh vykázalo 52,1 procenta obcí, podíl je ale dlouhodobě stabilní. Zadlužení krajů loni vzrostlo o tři miliardy korun na 24,8 miliardy. Vyplývá to z informací, které včera zveřejnilo ministerstvo financí. Na zadlužení obcí se z 32,4 procenta podílejí čtyři největší města, tedy Praha, Brno, Ostrava a Plzeň. Velikost jejich dluhu ale dlouhodobě klesá, loni činila 22,5 miliardy korun a meziročně se snížila o 5,3 miliardy. Celkový dluh Prahy loni činil 14,2 miliardy korun. Text a foto: ČTK

Lidé mohou volit prezidenta i z karantény

Praha – Příštího prezidenta zřejmě budou moci volit v lednu i lidé, kteří v té době budou v karanténě nebo izolaci kvůli koronaviru. Budou mít možnost hlasovat z auta na zvláštních stanovištích či do speciálních přenosných schránek. Sněmovna včera návrh zrychleně schválila. Souhlas musí dodat ještě Senát, který by tak mohl učinit koncem příštího týdne. **(čtk)**

Zloději líčí pasti. Touží po platebních kartách

Digitální podvody
Jak bránit své peníze

VILÉM JANOUŠ

Paní Kateřina si stáhla aplikaci, která převáděla psaný text do formátu PDF. Ve chvíli, kdy si ji stáhla, začaly ji chodit SMS za placené služby. Text zprávy oznamoval, že pokud chce služby zrušit, musí poslat SMS na níže uvedená čísla, což také udělala. Jenomže jedna taková SMS ji přišla na 99 korun. Přestože přestala na zasílané SMS reagovat, stále ji chodily a byly zpoplatněny částkou 99 korun. Paní Kateřina se stala oběti zneužití plateb prostřednictvím mobilního operátora a stálo ji to devět set korun.

„Platby přes operátora jsou bezpečnou a obecně rostoucí platební metodou, nicméně operátoři důrazně upozorňují, aby lidé byli při placení stejně obezřetní jako při používání platební karty. Tak jako se internetoví podvodníci snaží zneužít v podvržených aplikacích platební karty, zaměřují se i na zneužití m-plateb a premium SMS," řekl manažer segmentu plateb z O2 Lukáš Pohan.

Jen v síti tohoto operátora vzrostl za poslední tři roky počet transakcí čtyřnásobně, a proto se stále častěji obrací na tuto oblast i pozornost podvodníků.

„Problémy se zpravidla objevují po vylákání autorizačních kódů na sociálních sítích. V těchto případech útočník napadne profil a následně se snaží z kontaktů napadeného vylákat jejich telefonní číslo a potvrzovací SMS kódy pro provedení transakcí," uvedl Pohan. Škody se sice pohybují nejčastěji v řádu nižších stokorun a operátoři drtivou většinu reklamací uznávají, ale i tak to může zabolet. „Obecně platí princip nulové důvěry. Pokud se na vás na sociálních sítích obrátí váš známý nebo i člen rodiny se žádostí o přeposlání autorizačního kódu, nepředávejte jej. I kdyby se jednalo o skutečnou potřebu, zkuste se s tímto člověkem spojit jinou metodou, třeba mu zavolat. Případně jej upozornit na to, že jeho profil vám tyto požadavky posílá, aby mohl učinit nápravná opatření a získat zpět kontrolu nad svým účtem," doplnil Pohan.

Ale kyberzločinci líčí i jiné pasti, jak vylákat přístupové kódy k platebním kartám svých obětí. Například pomocí falešných platebních bran. Ty vyhlížejí jako skutečné stránky oficiálních institucí a okrádaný ani nemusí tušit, že zadávání svých údajů je předává zlodějům. „Podvrhnout stránku je velmi jednoduché a běžný uživatel to většinou nepozná," uvedl IT specialista společnosti BDO Marek Kovalčík.

Česká bankovní asociace tvrdí, že s podobnými podvody se setkává stále častěji. Odborníci proto nabádají k opatrnosti. Zbystřit by lidé měli třeba v případě, kdy se prodávajícímu ozve cizinec. Na pozoru by měli být i ti, kterým kupující nabízí nestandardní způsob dopravy nebo platby. Rozhodně by ale neměl prodávající reagovat na požadavky kupujícího, že zaplatí přes neznámé služby různých nebankovních platebních společností nebo v kryptoměně.

Jako užitečný návod, jak rozpoznat podvodné útoky, může posloužit Kybertest.cz, který připravila právě Česká bankovní asociace. V něm si každý může vyzkoušet svou zdatnost v kybernetické bezpečnosti.

Foto: Pixabay

www.denik.cz

E-paliva jsou poslední šancí pro klasická auta

dokončení ze strany 1

„Výroba je také velmi energeticky nákladná zejména kvůli získání recyklovaného uhlíku. Pokud trváme na bezemisní dopravě, bude potřeba syntetizovat paliva s využitím jaderných zdrojů stálého výkonu v kombinaci s občasnými obnovitelnými zdroji energie," upozornil Macek. Podle něho by tak bylo schůdnější přidávat syntetickou část do současných fosilních paliv a postupně její část zvyšovat.

Vývoj syntetických paliv už v reálu probíhá. Třeba automobilka Porsche ve spolupráci se společností Siemens plánuje do roku 2026 vyrábět zhruba 550 milionů tun e-paliva ročně.

Pro srovnání: podle odhadů se denně na celém světě spotřebuje až 100 milionů barelů ropy, jeden barel přitom váží něco přes sto kilogramů. Zatím se uměle vyrobená paliva komerčně neprodávají. Důvodem je vysoká cena, litr by stál na čerpacích stanicích odhadem tisíce korun.

Experti nicméně věří, že syntetická paliva jednoho dne budou řídiči tankovat do aut zcela běžně. **(elm)**

Na Polsko dopadly rakety. Jsou dva mrtví, tvrdí média

Varšava – Raketové útoky včera zasáhly i Polsko. Spadnout měl poblíž východních hranic s Ukrajinou. O ruském původu raket informovalo polské Radio ZET s odkazem na americké činitele tajné služby.

Podle americké agentury AP, která se rovněž dovolává na tajné služby, byly na místě dva mrtví. Dopady střel na území člena NATO potvrdil i litevský ministr obrany Artis Pabriks na svém Twitteru.

Polský premiér Mateusz Morawiecki svolal okamžitě krizový štáb. Premiérův mluvčí Piotr Müller apeloval na média, aby nepotvrzené informace nezveřejňovala. „Vyjádříme se k nim a budeme o nich informovat. Všechny informace, které budou na štábu řešeny, budou zpřístupněny veřejnosti. Pokud to bude možné, tak v maximální možné míře," řekl pro deník Gazeta Wyborcza Müller.

Rakety dopadly poblíž města Przewodów a zasáhly sušárnu obilí. Městečko leží poblíž ukrajinský hranic, severně od Lvova. Toto ukrajinské město se včera stalo terčem řady ruských raketových útoků. **(mk)**

České neziskovky převzaly Cenu evropského občana

Evropa pro Čechy

MARCEL MORŽOL

LAUREÁT. Kancléřkou Ceny evropského občana je místopředsedkyně Evropského parlamentu Dita Charanzová, která na snímku předává ocenění Evženu Adámkovi z Charity Znojmo. Foto: EP

Brusel – V Evropském parlamentu představila vzdělávací platformu HolkyZMarketingu jedna z jejích zakladatelek Pavlína Loučenská. Tuto možnost dostala pouze trojice z letošních 30 laureátů Ceny evropského občana. Ve většině členských zemí bývá každoročně oceněn jeden projekt. Česko však letos uspělo hned dvakrát a do Bruselu zamířili pro ocenění i zástupci Charity Znojmo.

Vzdělávací platforma HolkyzMarketingu se snaží pomáhat především ženám.

„Chceme zlepšit postavení žen na pracovním trhu," řekla Loučenská. Na své vzdělávací programy nabízí také stipendia.

Práci Charity Znojmo představil v Bruselu ředitel Evžen Adámek. Znojemská charita slaví letos 30 let a provozuje především zdravotní a sociální služby v regionu. Vedle toho ovšem dlouhodobě vyvíjí aktivity na Ukrajině. V posledních několika letech i přímo v Lysyčansku, přes který prošla fronta válečného konfliktu. „Na Ukrajině pomáháme přes 20 let. V roce 2015 jsme získali partnery z charity v Lysyčansku. Tam jsem začali vozit humanitární pomoc a podílet se na projektech v místě," říká Adámek. To vše změnila v únoru válka. Charita Znojmo začala pomáhat hned od začátku a velkou výhodu bylo právě to, že má na Ukrajině dlouhodobé partnery.

Cenu evropského občana uděluje Evropský parlament od roku 2008. V Česku se udílí od roku 2014. Cenu získávají jednotlivci a organizace v členských zemích, jejichž činnosti prohlubují vzájemné porozumění a spolupráci mezi občany. Letos se přihlásilo 300 iniciativ.

125. „Pro zboží si přijede kurýr.“ Podvod známý z bazarů vás může stát statisíce

Online ● seznamzpravy.cz (Zprávy / Politika) ● 16. 11. 2022, 8:41

Vydavatel: **Seznam.cz, a.s. (cz-26168685)** ● Autor: **Karolína Štuková**

Dosah: 1 702 492 ● GRP: 18.92 ● OTS: 0.19 ● AVE: 79177.75 Kč ● Interakcí: 266

Odkaz: https://www.seznamzpravy.cz/clanek/tech-technologie-pro-zbozi-si-prijede-kuryr-podvod-znamy-z-bazaru-vas-muze-stat-statisice-218608

ıam Zprávy

Ilustrační foto.

8:41

„Přijdou ti zprávy, kódy v nich mi napiš. Ok?“ Na první pohled nevinná zpráva může oběť internetového podvodu stát i statisíce korun.

Prodávali jste někdy něco na inzertních serverech? Potom si mohli podvodníci vyhlédnout i vás a vylákat podvodem vaše peníze. Přestože se jedná o celkem nový druh podvodu, internetoví uživatelé se s ním setkávají stále častěji.

Princip tohoto podvodu je jednoduchý. Podvodník získá z inzerátu e-mail nebo telefonní číslo uživatele a kontaktuje ho, většinou prostřednictvím aplikací WhatsApp nebo Messenger s předstíraným zájmem o koupi inzerovaného zboží. Během konverzace ho navádí k tomu, aby uhradil poplatek za přepravu zboží, kterou kupující (v tomto případě tedy podvodník) zajistí, a to přes platební bránu jím domluveného dopravce. V odkazu na falešnou platební bránu, který uživateli ve zprávě zašle, po něm chce vyplnit citlivé údaje o platební kartě včetně PIN, případně přístupové údaje do online bankovnictví včetně hesla a bezpečnostního kódu z autorizační SMS.

Díky získaným údajům se podvodník dostane do online bankovnictví oběti, kde provede převod finančních prostředků na svůj bankovní účet, nebo na základě zjištěných údajů z platební karty provede její tokenizaci a následně v bezkontaktním bankomatu vybere

z účtu peníze. Tak popisuje podvod krok za krokem Česká bankovní asociace.

Kampaň #nePINdej!

Patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti u nás. Zapojily se jak orgány státní správy, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají.

Kromě ČBA i Policie České republiky i Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), itego, a. s., Cisco, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy.

Mediálními partnery jsou Česká televize (hlavní mediální partner), Seznam Zprávy, Deník a CineStar.

Dosud jen pražští kriminalisté zadokumentovali celkem přes čtyřicet podobných případů se škodou v řádech milionů korun.

V letošním červnu zadrželi například dva cizince, kteří se v rámci organizované skupiny, která působí po celé Evropě, dopustili řady podvodů. Oba muži od poškozených osob vylákali pod různými záminkami údaje k jejich bankovním účtům. Na jejich základě vytvářeli virtuální platební karty a z účtů poškozených vybírali finanční částky od tisícikorunových položek až po statisíce. Tyto finanční prostředky ihned vkládali na své účty, případně ukládali do bitcoinmatů, uvedla Policie ČR na svých webových stránkách.

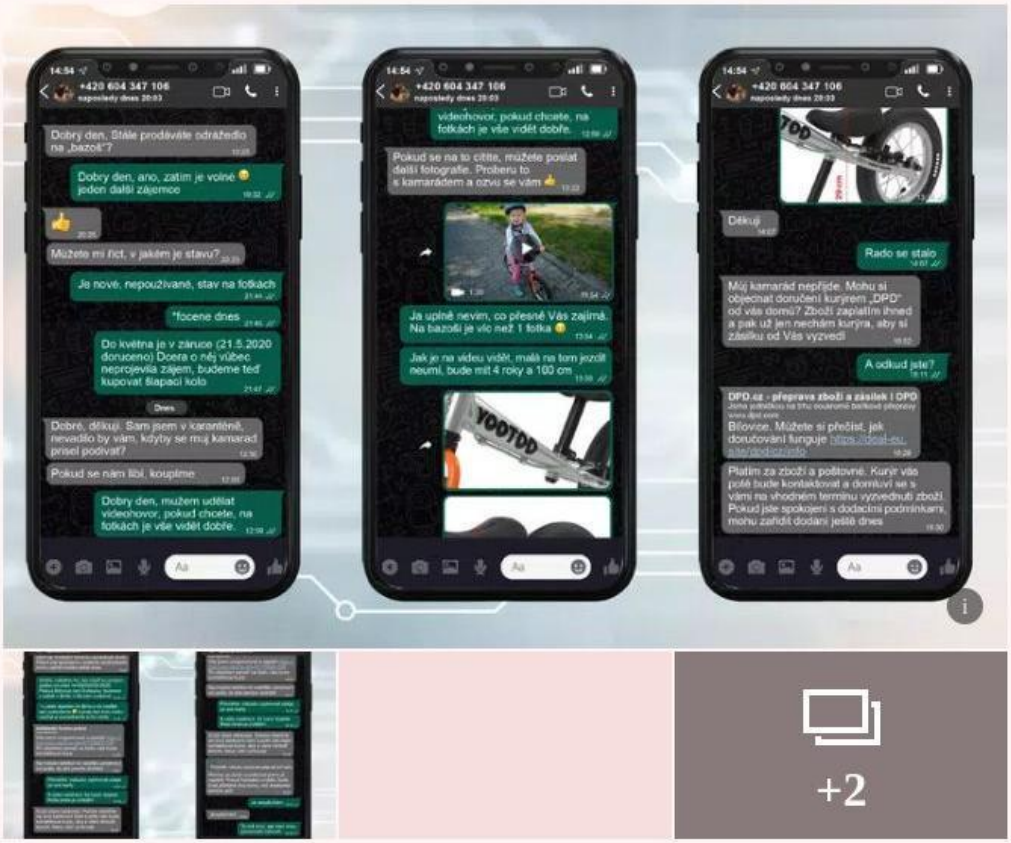
A postup byl jasný. K vylákání platebních údajů, informací z platebních karet a internetovému bankovnictví poškozených se spolupachatelé obou obviněných dostávali právě pod legendou fiktivních inzerátů o prodeji či koupi zboží na internetových portálech a díky falešně vytvořeným platebním bran finančních institucí.

Podle Michala Čarného, generálního ředitele společnosti Mastercard pro Česko a Slovensko s rostoucím objemem online transakcí, který ještě zesílil během pandemie covidu, úměrně

roste i počet pokusů o podvody.

„Pro většinu útoků platí, že jsou vedeny v co největším rozsahu a bývají obvykle automatizované," uvádí Čarný. „Objevují se ale i sofistikované útoky, kdy se útočníci snaží co nejvíce napodobit obvyklé lidské chování nebo se pokouší nakupujícího zmanipulovat či uvést v omyl," dodává.

Ukázka jak podvod může vypadat:



Obecně ale podle šéfa Mastercard platí, že platby kartou jsou v současnosti historicky vůbec nejbezpečnější. Je to proto, že dnes funguje celá řada nástrojů založených na datech a umělé inteligenci, které jsou schopny identifikovat a předejít zneužití karet kdekoliv na světě.

Riziko útoků ale ani přesto nezmizí. „Útoky budou sofistikovanější, rychlejší. Vidíme, že se mění i zaměření útoků. Už nyní jsme svědky posunu k útokům na firmy a jejich dodavatelské řetězce s cílem způsobit maximální škodu," dodává Michal Čarný.

Jak podvodné platební brány poznat a jak se jim bránit?

- Pokud na inzerát reaguje cizinec, zbystřete.
- Buďte na pozoru, když kupující požaduje nestandardní způsob dopravy nebo způsob platby. Příkladem je zajištění jeho platby „přepravní společností", která peníze uvolní, až bude zboží na cestě, nebo platební brána, která vyžaduje údaje z platební karty prodávajícího.
- Nereagujte na požadavky kupujícího, že zaplatí přes neznámé služby různých nebankovních platebních společností nebo v kryptoměně.
- Nepřistupujte na platbu nedoplatků, přeplatků či kaucí a nikam nezadávejte své platební údaje, například číslo karty. Kupující má platit vám, ne vy jemu.

Zdroj: ČBA, Kybertest

Ale nejsou to jen platební brány a citlivé údaje v nich, které by měly být uživatelem bezpečně střeženy. Jistou hrozbu představují také podvody páchané prostřednictvím zneužití plateb přes mobilního operátora. Na rozdíl od placení kartou ale v tomto případě nejsou peníze strženy z účtu, ale z předplaceného kreditu nebo měsíčního tarifu u mobilního operátora majitele telefonního čísla.

Platbou přes operátora je možné hradit různé internetové nákupy, ale i jízdenky na MHD, předplatná do aplikačních obchodů jako Google Play či App Store nebo nákupy spojené s herním průmyslem. Při využití plateb přes operátora nemusí uživatel prodejci poskytovat údaje o své platební kartě, ale nákup potvrdí jednorázovým kódem, který mu operátor pošle v textové zprávě.

Existují případy podvodů, které mají za cíl získat telefonní číslo, prostřednictvím kterého se

podvodník buď naboural do profilu uživatele na sociální síti, nebo napodobí profil někoho jiného a následně jménem této jiné osoby rozesílá zprávy do profilů v adresáři.

Pozor na podvod. Takhle vás okradou přes telefon

29. 10. 8:49

„Tento druh podvodů se stává a riziko s tím, jak se stále více dostáváme do on-line prostředí, roste. V tomto případě bych volil politiku nulové důvěry. Pokud se člověk setká s tím, že mu známý píše prostřednictvím účtu na sociálních sítích a požaduje po něm autorizační SMS nebo jakákoliv hesla, doporučuji rozhodně tyto informace nezasílat," vysvětluje za mobilního operátora O2 Lukáš Pohan, manažer segmentu plateb.

Typicky podle jeho slov podvodníci prostřednictvím napadených profilů vytvářejí na potenciální oběť jistou naléhavost, protože autorizační kódy mají omezenou platnost, často v řádu minut.

Celkově ale obliba mobilních plateb roste. Jen u O2 je za necelé 3 roky vidět nárůst unikátních uživatelů, kteří m-platbu používají opakovaně, na několikanásobek. Počet unikátních transakcí je pak více jak dvojnásobný.

Jak podvodné m-platby poznat a jak se jim bránit?

- Profily na sociálních sítích mějte zabezpečené dvoufázovým ověřením. Pokud by pachatel získal vaše přihlašovací údaje, musel by z vás vylákat ještě i autorizační kód.
- V případě, že vám někdo profil na sociální síti napadl, ihned kontaktuje zákaznickou podporu sociální sítě a okamžitě si změňte heslo.
- Na sociální sítě, do e-mailových profilů, do on-line bankovnictví apod. se přihlašujte pouze z oficiálních webových stránek.

- U sociálních sítí a v kyberprostoru v běžné písemné komunikaci obecně platí, že nikdy nevíte, s kým reálně komunikujete. Na to myslete pokaždé, když s někým takto komunikujete nebo pokud chcete odeslat citlivé údaje. Pro ověření identity protistrany raději využijte jiný komunikační kanál.
- Nikdy nikomu nesdělujte žádné kódy, které jste obdrželi, ať již v SMS, nebo jiným způsobem.

Zdroj: ČBA, Kybertest

Jak jsou na tom vaše znalosti základních principů bezpečného chování na internetu, si můžete vyzkoušet v online interaktivním kybertestu, který v rámci vzdělávací kampaně spustila Česká bankovní asociace.

Seznam Zprávy jsou mediálním partnerem **kampaně #nePINdej.**

126. Lidské chyby mohou za 90 procent kybernetických incidentů. Největší hrozbou je phishing

Online ● e15.cz (Zprávy / Politika) ● 16. 11. 2022, 10:10

Vydavatel: **CZECH NEWS CENTER a.s. (cz-02346826)**

Dosah: 76 245 ● GRP: 0.85 ● OTS: 0.01 ● AVE: 50000.00 Kč

Odkaz: https://www.e15.cz/tematicke-specialy/kyberneticka-bezpecnost/lidske-chyby-mohou-za-90-procent-kybernetickych-incidentu-nejvetsi-hrozbou-je-phishing-1392732

Lidské chyby mohou za 90 procent kybernetických incidentů. Největší hrozbou je phishing

Hackeři a útočníci, kteří ovládají sociální inženýrství, jsou hrozbou pro citlivá firemní data. Například 52 procent všech phishingových útoků z prvního pololetí 2022 se odehrálo na profesní síti LinkedIn. Manipulaci zaměstnanců se dá předejít pouze pravidelným školením a správným nastavením technologických pravidel a opatření.

Sociální inženýrství je jedním z nejčastějších způsobů, jakým se útočníci zmocňují citlivých firemních dat. Promyšlenými nástrahami například manipulují zaměstnanci, kteří jim pak nevědomky umetou cestu k nebezpečnému útoku. Stačí jim k tomu využít důvěry, naivity a neznalosti.

Útok cílený přes lidi nevyžaduje tolik finančních ani hackerských schopností. Je to však druhý nejvyužívanější způsob ataku, který ročně okrade firmy o miliardy dolarů. Bránit se proti němu je nesmírně obtížné a vyžaduje to komplexní přípravu, která obsahuje lidi i technologie. Manažer dohledového centra O2 Jiří Sedlák vysvětluje, že ke kybernetické bezpečnosti je nutné přistupovat komplexně. *„Moje doporučení je školit, ale zároveň nasazovat další technologická a procesní pravidla a opatření. Dále pak konzultovat situaci ve své firmě s odborníky na bezpečnost."*

Druhy útoků s využitím sociálního inženýrství

Útočníci využívají mnoho způsobů, jak se k datům dostat. Aktuálně největším strašákem je tzv. **phishing**, při kterém se **útočník vydává za důvěryhodné organizace**, banky, přepravní společnosti nebo obchodní partnery a snaží se z obětí vylákat nejrůznější informace. Může to dělat přes email, SMS, sociální sítě nebo přes hovor (pak se používá výraz vishing). Útočník se snaží vyvolat dojem, že protistrana něco chce nebo potřebuje.

Problematická je z tohoto pohledu i profesní síť LinkedIn. Právě tato síť se pyšní nelichotivým prvenstvím – 52 procent všech phishingových útoků z prvního pololetí 2022 se odehrálo právě zde. Ukazuje to analýza společnosti AtlasVPN. Útočníci při svých nekalých praktikách zneužívají to, že používá automatické zkracování URL adres na 26 znaků a vystavený příspěvek na síti může odkazovat kamkoliv a přes několik přesměrování se uživatel ocitne na phishingové stránce.

Haló, jaký je váš PIN?

Jak již bylo zmíněno, útočníci často využívají i běžné telefonické hovory. Scénář vypadá nejčastěji takto: Na displeji telefonu se objeví číslo klientské linky vaší banky a na druhé straně se ozve údajný zaměstnanec, který naléhavým tónem sděluje, že hrozí ztráta peněz na vašem účtu. Další část příběhu pokračuje tak, že je možné peníze zachránit tím, že sdělíte své přihlašovací údaje k internetovému bankovnictví, nadiktujete volajícímu údaje z platební karty, nebo je sami aktivně převedete na jiný účet. Jeho číslo vám nyní váš zachránce ochotně nadiktuje. Ano, tak jednoduché to bohužel je.

Jak vyplývá z dat České bankovní asociace (ČBA), počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně. Škody jdou do stovek milionů a na jednoho

poškozeného klienta je to v průměru 161 500 korun. ČBA proto ve spolupráci s orgány státní správy a s klíčovými firmami českého byznysu spouští rozsáhlou celonárodní vzdělávací kampaň #nePINdej! Ta má za cíl varovat a preventivně chránit před kybernetickými bankovními podvody, například formou Kybertestu.

Jak se útokům bránit

Útočníci vždy začínají pečlivým shromažďováním informací a budováním důvěry, kterou následně zneužijí a na závěr z obětí vylákají peníze, nebo ukradnou informace, které pak prodají. Je proto nezbytné neustále opakovat základní pravidla. Lidé by **neměli otevírat emaily z neznámých adres a v žádném případě podezřelé přílohy**. Měli by **používat silná hesla a dvoufázová ověření**. Důležité je také **nepoužívat neznámé USB disky nebo nezaheslovaná úložiště**.

Jak vysvětluje ředitel útvaru bezpečnosti O2 Radek Šichtanc, pouhé vyškolení obvykle nestačí: *„I zkušený a vzdělaný uživatel může udělat chybu. Včetně admina po 20 letech v IT bezpečnosti. O to horší ta chyba může být. Proto je důležitá záchranná brzda v podobě bezpečnostních nástrojů, automatizovaných technologií, bezpečnostního monitoringu atp."*

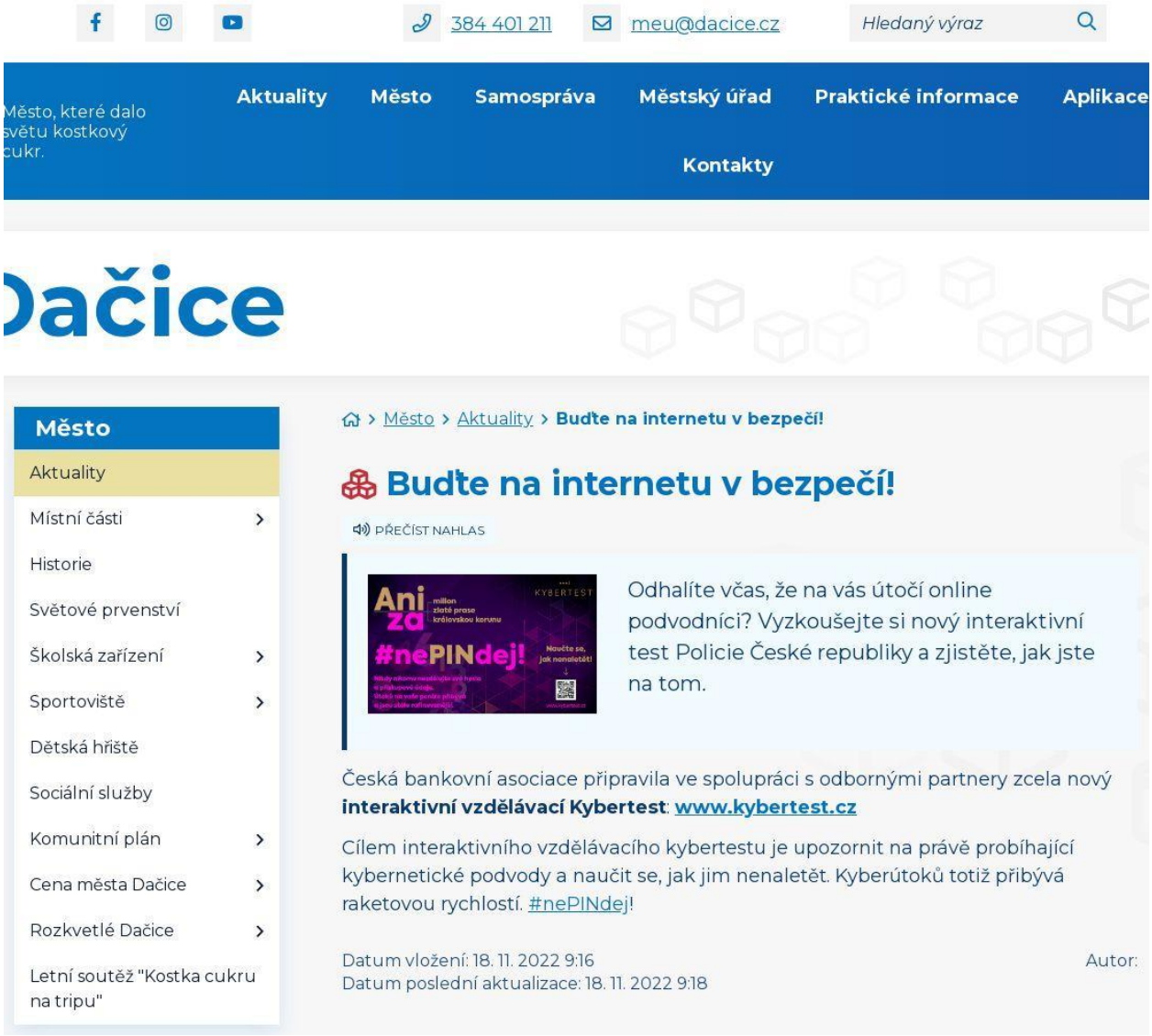
Tematický speciál Kybernetická bezpečnost připravuje E15 ve spolupráci s O2.

127. Buďte na internetu v bezpečí!

Online ● dacice.cz ((nezařazené)) ● 18. 11. 2022, 9:16

Dosah: 1 345 ● GRP: 0.01 ● OTS: 0.00 ● AVE: 6277.49 Kč

Odkaz: https://www.dacice.cz/mesto/aktuality/budte-na-internetu-v-bezpeci-4301cs.html



128. Zloději líčí pasti. Zneužívají prémiové SMS a touží po platebních kartách obětí

Online ● havlickobrodsky.denik.cz (Regionální zprávy) ● 19. 11. 2022, 11:15

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)** ● Autor: **Vilém Janouš** ● Rubrika: **Zprávy**

Dosah: 965 223 ● GRP: 10.72 ● OTS: 0.11 ● AVE: 852228.93 Kč

Odkaz: https://havlickobrodsky.denik.cz/zlociny-a-soudy/falesne-platebni-brany.html

On-line nákupy | *Foto: Shutterstock*

Paní Kateřina se stala obětí zneužití plateb prostřednictvím mobilního operátora a stálo jí to devět set korun. „Platby přes operátora jsou bezpečnou, obecně rostoucí platební metodou – v cizině i Česku, nicméně operátoři důrazně upozorňují, aby lidé byli při placení stejně obezřetní jako při používání platební karty. Navštěvujte prověřené internetové stránky a stahujte jen prověřené aplikace z oficiálních aplikačních obchodů Google a Apple. Tak jako se internetoví podvodníci snaží zneužít v podvržených aplikacích platební karty, zaměřují se i na zneužití m-plateb a premium SMS," upozornil manažer segmentu plateb společnosti O2 Lukáš Pohan.

Popularita těchto plateb obecně roste. Jen v síti O2 vzrostl za poslední tři roky počet transakcí čtyřnásobně. Nejčastěji takto lidé platí za různé aplikace a hry, audiovizuální služby nebo za přístup k elektronickým informacím, magazínům a knížkám.

Množí se telefonáty od falešných bankéřů. Lidé mohou přijít o statisíce

PŘEČÍST ČLÁNEK ›

Právě kvůli rostoucí oblibě tohoto typu plateb se na něj ale stále častěji zaměřují i podvodníci. „Často se objevují případy vylákání autorizačních kódů na sociálních sítích. V těchto případech útočník napadne profil na sociální síti a následně se snaží z kontaktů napadeného vylákat jejich telefonní číslo a potvrzovací SMS kódy pro provedení transakcí," uvedl Pohan.

Škody se sice pohybují nejčastěji v řádu nižších stokorun a operátoři drtivou většinu reklamací uznávají, protože si poté vše řeší s dodavateli obsahu, ale i tak je to pro oběti podvodníků velmi nepříjemné. „Obecně platí princip nulové důvěry, to znamená, pokud se na vás na sociálních sítích obrátí váš známý nebo i člen rodiny se žádostí o přeposlání autorizačního kódu, nepředávejte jej. I kdyby se jednalo o skutečnou potřebu, tak se zkuste s tímto člověkem spojit jinou metodou, například mu zavolat a prověřit si, že s vámi jednal skutečně on. Případně jej upozornit na to, že jeho profil na sociální síti vám tyto požadavky posílá, aby mohl případně učinit nápravná opatření a získat zpět kontrolu nad svým účtem," doplnil Pohan.

Případ falešných platebních bran

S rozvojem internetových služeb a plateb už zločinci zpravidla nevyčkávají na svou oběť někde na ulici, ale číhají v online světě. Kromě jiného také líčí pasti, kterými se snaží vylákat přístupové kódy k platebním kartám svých obětí. Například pomocí falešných platebních bran. Ty vyhlížejí jako skutečné stránky oficiálních institucí, a oběť proto často netuší, že zadáváním svých údajů je předává zlodějům.

„Vytvořit podvrh, který vypadá stejně jako určitá stránka, je velmi jednoduché a běžný uživatel to většinou nepozná. Klíčové je vždy vědět, že doopravdy dělám operaci, kterou jsem chtěl," míní například IT specialista společnosti BDO Marek Kovalčík.

Generální ředitel společnosti Mastercard pro Českou republiku a

Nový seriál Deníku: Digitální podvody. *Zdroj: Deník*

Slovensko Michal Čarný k tomu uvedl, že útoky bývají zpravidla automatizované. „Objevují se ale i sofistikované útoky, kdy se útočníci snaží co nejvíce napodobit obvyklé lidské chování nebo se pokouší nakupujícího zmanipulovat či uvést v omyl," uvedl Čarný.

Česká bankovní asociace tvrdí, že s podobnými podvody se setkává stále častěji. Zloději si například vyhlédnou někoho, kdo něco prodává na inzertním serveru. Na nich pak podvodníci získají e-mailovou adresu nebo telefonní číslo své oběti. Prostřednictvím aplikací Whatsapp nebo Messenger následně předstírají zájem o koupi zboží a nabádají svou oběť, aby uhradila poplatek za přepravu zboží, kterou útočníci zajistí.

Následně pošlou odkaz na falešnou platební bránu přepravní společnosti, v níž má prodávají vyplnit citlivé údaje o platební kartě včetně PIN, případně přístupové údaje do online bankovnictví včetně hesla a autorizačního kódu z SMS. Díky tomu se pak útočník dostane do online bankovnictví své oběti.

SMS nebo e-mail. Zprávy od hackerů umí nepozorné připravit o desetitisíce korun

PŘEČÍST ČLÁNEK ›

Odborníci proto nabádají k opatrnosti. Zbystřit by lidé měli třeba v případě, kdy se prodávajícímu ozve cizinec. Na pozoru by měli být i ti, kterým kupující nabízí nestandardní způsob dopravy nebo platby. Rozhodně by prodávající neměl reagovat například na požadavek, že kupující zaplatí přes neznámé služby různých nebankovních platebních společností nebo v kryptoměně.

„Nepřistupujte na platbu nedoplatků, přeplatků či kaucí a nikam nezadávejte své platební údaje, například číslo karty. Kupující má platit vám, ne vy jemu," nabádá bankovní asociace.

Jako užitečný návod, jak rozpoznat podvodné útoky, může posloužit Kybertest.cz, který připravila právě Česká bankovní asociace. V něm si každý může vyzkoušet svou zdatnost v kybernetické bezpečnosti.

129. Prevence bude hrát v bezpečnosti prim, říká Irena Hýsková (Thein Security)

Tisk ● Security World; str. 10, 11 (IT / Technologie) ● 21. 11. 2022

Vydavatel: **Internet Info DG, a.s. (cz-00565211)** ● Rubrika: **Partnerský příspěvek**

Dosah: 18 000 ● GRP: 0.20 ● OTS: 0.00 ● AVE: 170000.00 Kč

Odkaz: náhled

Partnerský příspěvek

Prevence bude hrát v bezpečnosti prim, říká Irena Hýsková (Thein Security)

Jaké jsou současné výzvy v oblasti kybernetické bezpečnosti, vysvětluje Irena Hýsková, výkonná ředitelka společnosti Thein Security, společně se svými kolegy Ondřejem Remešem, cyber security managerem, Oldřichem Gosmanem, manažerem pro SOC.

V poslední době se stále častěji mluví o nové evropské bezpečnostní směrnici NIS2. Co mohou firmy od ní očekávat?
Irena Hýsková (IH): NIS2 navazuje na předchozí evropskou normu NIS z roku 2016. Cílem je zvýšit kybernetickou odolnost firem kritické infrastruktury a také dalších významných podniků, a to zejména v oblasti prevence. Lze čekat, že se dotkne přibližně šesti tisíc soukromých i státních subjektů.

Mezi možná preventivní opatření patří např. kontinuální školení zaměstnanců, kvalitní firewally, zabezpečení koncových zařízení, vícefaktorové ověřování nebo produkty antiDDoS. Řešení existuje celá řada, a naše firma má tým, který je dokáže aplikovat.

NIS2 také představuje vyšší odpovědnost statutárních orgánů jednotlivých společností a na rozdíl od NIS se zaměřuje právě na zmíněnou prevenci. Doporučuji každému zodpovědnému manažerovi sledovat stránky úřadu NÚKIB pro nejaktuálnější vývoj.

Hrozí v rámci NIS2 firmám nějaké sankce?
IH: Určitě ano, směrnice navíc stanovuje maximální hranice pokut poměrně vysoko (v max. výši deset milionů eur nebo dvě procenta ze světového obratu). NÚKIB na svých stránkách také uvádí, že lze očekávat proporcionální pokuty zohledňující povahu porušení, hrozící škody apod. Firmy by se tedy měly zamyslet nad tím, co jim může nesplnění požadavků NIS2 přinést. Nejde jen o finanční sankce, ale především o dopad případného kybernetického útoku na samotnou organizaci (ztráta firemní reputace, dat, výpadek provozu výrobních kapacit aj.).

Jsou firmy podle vás schopné požadavkům NIS2 vyhovět svépomocí?
IH: K NIS2 budou určitě vydané metodické pokyny k jejímu naplňování. Jde však stejně jako u účetnictví o složitou problematiku.

Irena Hýsková

Zastává pozici CEO ve společnostech Thein Security a Cybersecurity Guard, kde má na starosti naplnění bezpečnostní strategie, zavedení bezpečnostního dohledového centra SOC, finanční a provozní řízení a definici prodejní strategie.

Firmy mají zákonnou povinnost účetní agendu vést a zároveň ji potřebují ke svému podnikání. A podle složitosti účetní agendy volí, jestli se jí budou zabývat samy, zaměstnají interního specialistu nebo najmou externí, specializovaný subjekt.

Ne každá společnost si ale může dovolit vlastní tým odborníků na kybernetickou bezpečnost, tak aby si mohly všechny oblasti tohoto oboru pokrýt vlastními silami. V každém případě tedy doporučuji kontaktovat specializované firmy, které se kybernetickou bezpečností zabývají, a přinejmenším s nimi zkonzultovat vlastní plány na implementaci NIS2.

Existují nástroje, které by firmám pomohly splnit zvýšené požadavky na ochranu dat, aniž by musely zaměstnávat množství bezpečnostních expertů?
IH: Je zjevné, že na trhu práce právě tato specializace dlouhodobě chybí. Automatizace v oblasti detekce a reakce na bezpečnostní události – systémy SOAR – je dnes jedna z mála šancí, jak potřebu na velké množství lidí v oblasti kybernetické bezpečnosti nějak snížit.

Naštěstí existují firmy, mezi něž patří i ta naše, které nedostatek expertů dokážou vhodně doplnit nástroji renomovaných společností.

Thein Security spolupracuje například s Palo Alto Networks, u níž je držitelem nejvyšší dodavatelské certifikace Diamond Innovator a je jediným autorizovaným servisním centrem pro ČR/SR, dále s firmami Netscout, Microsoft a dalšími. A od společnosti PANW máme v portfoliu například Cortex XDR, což je produkt, který detekuje i vyšetřujte případné hrozby a nežádoucí aktivitu dokáže zastavit v reálném čase.

Dalším vhodným řešením je NGFW, proaktivní nástroj umožňující hloubkovou kontrolu provozu včetně šifrované komunikace na úrovni síťového provozu, aplikací, uživatelů a obsahu přenášených dat. Umožňuje tak předcházet známým i neznámým hrozbám. A od společnosti Netscout pak nabízíme řešení antiDDoS Arbor, které se globálně používá v malých i velkých firmách.

Organizační bezpečnost ale může mít na celkové zabezpečení firem větší vliv než použité technologie, je to tak?
Ondřej Remeš (OR): To je pravda, ale systémy řízení informační bezpečnosti – ISMS – jsou výsadou převážně velkých firem,

případně organizací, které potřebují prokázat soulad se standardy ISO 27000 nebo se zákonem o kybernetické bezpečnosti (ZoKB). V menších firmách je bohužel zatím dobrovolná adopce těchto standardů spíše výjimkou. Často je to také doprovázeno nedostatkem bezpečnostního personálu. Zároveň však vnímáme trend stále častějšího vzdělávání zaměstnanců a následného ověřování znalostí pomocí simulovaných phishingových kampaní. I to je aktivita, kterou se snažíme u našich zákazníků adresovat a pomoci vyřešit.

Osvěta je určitě klíčem k lepší bezpečnosti – co ale kromě školení může zlepšit obecné povědomí o kybernetické ochraně?

OR: Podle naší zkušenosti má smysl jen průběžné školení zaměstnanců, které posouvá jejich znalosti, ale zároveň nevyžaduje hodiny před monitorem. Důležitá je i zpětná vazba formou testů, kvízů nebo simulovaných phishingových kampaní, které prokážou aktuální úroveň znalostí a mohou ovlivnit strukturu a cílení školicího plánu. Stěžejní je také komunikace v organizaci. Motivace pro jednotlivce je různá a je důležité pochopit, že znalosti jsou k užitku také v soukromí. Pro širokou veřejnost pak existují formy testů nebo školení pořádané neziskovými nebo profesními organizacemi. Příkladem může být Kybertest.cz organizovaný Českou bankovní asociací, který za přispění Thein Security cílí na bezpečné používání elektronického bankovnictví.

Proč ale i vyškolení lidé útokům kyberzločinců dokážou podlehnout?

OR: I když člověk prochází takovým školením – a jak jsem zmínil, to je kontinuální proces – tak se může stát, že nerozpozná pokus o hackerský útok. Nicméně toto riziko se s pravidelnou edukací výrazně redukuje. V kyberbezpečnosti bohužel žádné opatření nedává jistotu, že k úspěšnému útoku nedojde. Právě dobře nastavené firemní procesy, existující bezpečnostní monitoring v rámci střediska bezpečnostních operací (SOC) a kontinuální vzdělávání s velkou pravděpodobností zaručí, že útok bude buď neúspěšný, nebo se včas a rychle objeví i vyřeší.

Právě phishing a sociální inženýrství představují hrozbu, proti kterým se špatně brání. Jaké by měly být zásady, jak jí čelit?

Oldřich Gosman (OG): Na phishingovou kampaň nepotřebujete žádné sofistikované nástroje, zjednodušeně řečeno vám stačí jen e-mail. Je mnohem snazší a levnější při útocích překonávat „běžný" lidský faktor a namísto prolamování bezpečnostních technologií si o citlivé informace jednoduše říct.

O Thein Security

Thein Security, součást skupiny Thein, nabízí komplexní služby spojené s ochranou firem v kyberprostoru včetně prevence úniku citlivých dat, obrany proti sofistikovaným útokům, detekce neznámého malwaru nebo aktivní ochrany proti DDoS útokům. Firma má vlastní bezpečnostní středisko SOC pro zákazníky, kteří se chtějí soustředit na své podnikání, ale současně vyžadují prvotřídní dohled nad ochranou svých dat v kyberprostoru.

Phishing se ale v dnešní době už netýká jen e-mailu, stejné riziko číhá i v případě tzv. instant messagingu, např. skrze Facebook Messenger, WhatsApp apod. Přes tyto platformy se šíří podvodné zprávy – i zdánlivě od přátel – vyzývající třeba k přeposlání citlivých informací, kliknutí na falešný odkaz či přílohu.

Phishing využívá známé životní situace, kdy útočník chce od uživatele získat cenné informace. A ty zásady? **Vzdělávejte se** – naučíte se, jak chránit sebe a svoji firmu. **Sdílejte na internetu co nejméně informací.** Dnešní útoky jsou vizuálně bezchybné, gramaticky správné a mají cílený, přesvědčivý obsah jak z hlediska technického, tak i psychologického. Chraňte své účty a zařízení silnými hesly – **používejte MFA**, tedy dvoufázová ověření pomocí kódu v SMS nebo otisku prstu.

Firmám, které mají problémy s vlastním zajištěním bezpečnosti, mohou pomoci SOC – střediska bezpečnostních operací. Co všechno může SOC zajistit a jak je to finančně náročné?

OG: SOC zájemcům doručí komplexní dodávku školených odborníků – SOC analytiků, technologií – dohledové nástroje typu XDR, EDR, SIEM, XSOAR a procesů. Také definují spolupráci a formalizují postupy v případě nálezů, incidentů a detekcí. Je to vlastně takový mix organizačních a technických opatření s cílem snížit útočnou plochu a detekovat anomálie. Finanční náročnost je pak závislá na požadavcích – některé firmě stačí dohled v pracovní dobu v režimu 5 × 8, jiná zase požaduje plný dohled 24 × 7 × 365, a to je cenově jiná služba.

Není pro firmu složité využít služby SOC?

OG: Složité to není, ale nejde o prostou „instalaci" technologií. Je to proces, který se vyvíjí s měnícími se potřebami zákazníka a bezpečnostní situací. Podle mne je klíčové prvotní rozhodnutí. V ideálním případě je k dispozici technická role, např. jde o architekta bezpečnosti a bezpečnostního ředitele, někoho s rozhodovací kompetencí.

V rámci našeho standardního postupu je klíčový tzv. onboarding, kdy se udělá vstupní analýza, definuje výchozí stav a zmapují aktiva firmy. Na to navazuje pilotní provoz SOC, definují se bezpečnostní alerty a jejich řešení. Tato fáze je na součinnost obou stran nejnáročnější. Ve všech těchto činnostech jsme v rámci best practice schopní firmám pomoci, ale finální rozhodnutí bude vždy na vlastníkovi. Výsledná opatření musejí podporovat procesy firmy a zároveň respektovat bezpečnostní požadavky – ani jeden ze zmíněných pohledů by neměl převažovat.

130. #nePINdej! Nová kampaň upozorňuje na časté internetové podvody

Online ● regionivancicko.cz (Regionální zprávy) ● 21. 11. 2022, 4:20

Dosah: 381 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 3138.95 Kč

Odkaz: https://www.regionivancicko.cz/zpravy/aktualne/21501--nePINdej-Nova-kampan-upozornuje-na-caste-internetove-podvody.html

Regionální zpravodajství

#nePINdej! Nová kampaň upozorňuje na časté internetové podvody

Krajské ředitelství policie Jihomoravského kraje
dnes 21.11.2022

Ilustrační foto
Autor: dreamstime.com

Počet útoků na klienty bank se za poslední dva roky **zvýšil čtyřnásobně.** Škody jdou do stovek milionů. Police ČR se připojuje k rozsáhlé vzdělávací kampani **#nePINdej!** České bankovní asociace a dalších partnerů, která upozorňuje na sílící nebezpečí podvodů na internetu.

Jak vyplývá z dat České bankovní asociace získaných od jejích členských bank, na jednoho poškozeného klienta připadá **průměrná škoda ve výši 161 500 korun**. U vishingu, neboli případů podvodného navolávání, jsou částky až **čtvrtmilionové.**

Klíčovým prvkem kampaně s názvem #nePINdej! (kreativní tvorba ze slov PIN nedej) je interaktivní vzdělávací www.kybertest.cz, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim předcházet.

Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. Kybernetická kriminalita již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se **zaměřují na širokou veřejnost bez ohledu na věk či vzdělání.** Kampaň proto cílí na širokou veřejnost počínaje dětmi a mladistvými přes dospělé až po seniory. Otázky v testu jsou tedy generovány dle věku uživatele. Na tvorbě kybertestu se podílela společnost Itego, a. s.

V kybertestu jsou **simulovány podvodné SMS, zobrazovací okna k připojení k WIFI sítím, phishingové emaily, zvukové nahrávky podvodných telefonů a mnohé další,** tak, aby si je každý uživatel moderních technologií mohl bezpečně vyzkoušet. Testové otázky byly připravovány odborníky na základě reálných případů, jimiž se podvodníci snaží své oběti nachytat.

Pachatelé se při těchto útocích snaží překonávat zejména lidský faktor a pod nejrůznějšími legendami využívají nátlaku, strachu a časové tísně pro záchranu peněz nebo pro realizaci finanční transakce.

Mezi nejčastější podvodné legendy patří:

1) Podvodné navolávání:

Nejčtenější v rubrice Aktuálně

Krok k privatizaci? Z nemocnic v Tišnově a Ivančicích má být akciová společnost

Výstavba Domova pro seniory v Ivančicích byla slavnostně započata

Na zdravotním středisku v Dolních Kounicích bude působit nová lékařka

Výzva 10 tisíc kroků pro zdraví: Zapojte se za Dolní Kounice

Rozvoj Dolních Kounic bude nadále pokračovat

Přidejte si **zprávy z regionu** na hlavní stránku Seznam.cz

Nejoblíbenější v rubrice Aktuálně

Rozvoj Dolních Kounic bude nadále pokračovat

Krok k privatizaci? Z nemocnic v Tišnově a Ivančicích má být akciová společnost

Dotace na energetický management pomůže Dolním Kounicím s úsporami

Výstavba Domova pro seniory v Ivančicích byla slavnostně započata

ZŠ TGM Ivančice se postupně digitalizuje

Kalendář akcí

1) Podvodné navolávání:

Pachatelé se vydávají například za bankéře, policisty, pracovníky technické podpory a snaží se z lidí pod vlivem strachu vylákat peníze, nebo vzdálený přístup do zařízení oběti, který následně zneužijí.

2) Nabídka výhodných investic:

Přesvědčivá lákavá reklama a manipulativní jednání. Cílem pachatele je vylákat z oběti co možná nejvíce finančních prostředků a využívá k tomu přirozenou ziskuchtivost každého z nás.

3) Reverzní inzertní podvody:

Pachatel zareaguje na váš inzerát. Podstrčí vám fiktivní platební bránu, kde vyplníte citlivé bankovní údaje a místo peněz za inzerované zboží přicházíte o všechny úspory.

4) Podvody typu Nigerijské dopisy:

Princip, který funguje už více jak 100 let. Pachatelé sázejí na kvantitu. Vždy se najde někdo, kdo se nechá nachytat na slibovanou cennou zásilku nebo domnělou pomoc. Často zde hraje velkou roli láska.

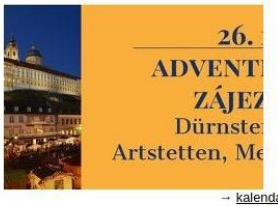
5) Klasické podvody typu phishing a smishing:

Stále dokonalejší a složitě rozpoznatelné podvodné emaily a SMS nabídky. Na první pohled již nenajdeme podezřelé znaky.

Stále častější praktikou jsou v současné době tzv. reverzní inzertní podvody. Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví. Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě **spolupracují a vyplňují údaje o svých kartách a přístupech na účet** v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou.

Základní rady, jak nenaletět

- Poznej svého nepřítele.
- Seznamuj se s aktuálními hrozbami a trendy v online podvodech.
- Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli.
- Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.
- Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze.
- Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.
- Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.
- Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.
- Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.



→ kalendář akcí

Co se děje v okolí

Pozor na změnu hromadné dopravy v Pohořelicích. Autobus do Mikulova vynechá několik zastávek

Linka 105 (Brno - Mikulov), pouze spoje 13 a 10 pojedou mezi zastávkami Pohořelice, Velký Dvůr a Pohořelice, Nová Ves obousměrně odklonem po silnicích II/381, I/52 a III/39616. Budou tak zcela vynechávat zastávky Pohořelice, Mariánský…

Zmatek v Hustopečích. Ve frontě na zubaře čekaly od rána stovky lidí

Centrem Hustopečí se táhla dlouhá fronta, jeden z místních zubařů nabíral nové pacienty. Někteří zájemci před ordinací dokonce nocovali.

131. Pozor na veřejnou Wi-Fi. Může se dívat podvodník

Tisk ● Tachovský deník; str. 6 (Regionální zprávy) ● 24. 11. 2022

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)**

Dosah: 542 613 ● GRP: 6.03 ● OTS: 0.06 ● AVE: 986470.47 Kč

Odkaz: náhled

6 Deník www.denik.cz 24. listopadu 2022

UDÁLOSTI

24 hodin na Ukrajině

Zásah porodnice. Zemřel dvoudenní chlapeček

Kyjev – Ruská raketa v noci na včerejšek zasáhla porodnické oddělení nemocnice ve Vilňansku, v Záporožské oblasti na jihu Ukrajiny. Zranění byli dva lékaři, jeden z nich je ve vážném stavu. Zahynul chlapeček, který se narodil přede dvěma dny, upřesnila ukrajinská prezidentská kancelář podle agentury Unian. Ukrajinská média s odvoláním na úřady také informovala, že dva lidé přišli o život a další dva utrpěli zranění včera ráno při ruském ostřelování Kupjansku v Charkovské oblasti na severovýchodě Ukrajiny. V Doněcké oblasti na východě země ruská palba během úterka zabila jednoho civilistu u Bachmutu, dalších osm bylo zraněno. Na fotografii zasažená porodnice ve Vilňansku.

CO SE TAKÉ VČERA STALO

ÚTOKY NA INFRASTRUKTURU I CIVILISTY. Po včerejším ruském raketovém útoku se obyvatelé hlavního města Ukrajiny ocitli bez vody a elektrického proudu. Ve městě panuje mrazivé počasí, uvedla agentura Unian. Ruské útoky v ukrajinské metropoli podle úřadů mimo jiné zasáhly také obytnou budovu, zemřeli nejméně tři lidé a šest dalších je zraněných. Exploze včera hlásily Oděská a Mykolajivská oblast na jihu Ukrajiny a Záporožská a Dněpropetrovská oblast na jihovýchodě.

DĚTSKÉ OBĚTI. Ve válce, kterou rozpoutalo Rusko vpádem vojsk na Ukrajinu před 274 dny, přišly podle ukrajinských úřadů o život již stovky dětí. Úřad vysoké komisařky OSN pro lidská práva potvrdil, že ve válce bylo zabito nejméně 415 dětí, ale připouští, že tyto údaje nejsou úplné a že skutečný počet obětí bude vyšší.

REZOLUCE. Europoslanci schválili rezoluci, ve které označují Rusko za stát podporující terorismus kvůli jeho útokům na ukrajinské civilisty.

Dění na Ukrajině sledujeme online

Pozor na veřejnou Wi-Fi. Může se dívat podvodník

Na veřejné Wi-Fi není radno používat elektronické bankovnictví či jakkoliv pracovat s osobními údaji.

Digitální podvody

Jak bránit své peníze

VILÉM JANOUŠ

Pan Jaroslav se přihlásil do veřejné Wi-Fi sítě. Přes ni se proklikal až na stránku, která vyhlížela jako reálný e-shop. Objednal si zboží a rozhodl se rovnou zaplatit. Stránka ho následně přesměrovala na platební bránu, v níž vyplnil všechny požadované údaje a zaplatil. Jenomže to byl podvod, což pan Jaroslav poznal ve chvíli, kdy mu backeři ukradli z karty peníze až do jejího limitu. Ve veřejné Wi-Fi síti totiž nikdo neví, kdo do vašeho soukromí zrovna nahlíží.

„Nikdy nevíte, kdo veřejnou síť skutečně provozuje a jaké má úmysly. U přístupu na webové stránky, které nepoužívají šifrování, může dojít velmi snadno k odchycení celé komunikace, tedy všeho, co si na dané webové stránce uživatel prohlíží, odesílá nebo třeba jaké vyplňuje osobní údaje," upozornil Jan Pinta ze společnosti Thein Security, která se zabývá kybernetickou bezpečností.

ČEŠI JSOU NEOPATRNÍ

Češi ovšem nejsou na svoje soukromí zrovna háklivi. Průzkum společnosti Anect ukázal, že veřejné sítě využívají tři čtvrtiny Čechů. Dvě třetiny z nich je používají k e-mailové komunikaci a jedna třetina dotázaných dokonce k internetovému bankovnictví.

„Pro útočníky je přitom velmi snadné, aby buďto ovládli nechráněnou veřejnou Wi-Fi například v hotelu, nebo, což je pro ně úplně nejjednodušší varianta, aby postavili svoji vlastní Wi-Fi například s názvem některé z oblíbených restaurací. Návštěvníci si potom neuvědomují, že pokud nepoužívají automaticky všude ochranu pomocí šifrování, první část jejich komunikace, která směřuje na tuto podvodnou Wi-Fi, je pro útočníka kompletně čitelná," uvedl expert na kybernetickou bezpečnost ze společnosti Anect Ivan Svoboda.

Jan Pinta z Thein Security upozornil na to, že falešné veřejné sítě se často mohou vydávat za na první pohled známé sítě, přičemž se jedná pouze o další podvod a nalákání oběti. „Na veřejných sítích se také často objevuje snaha o vylákání údajů k platební kartě nebo k instalaci softwaru, který následně komunikaci odposlouchává," doplnil expert.

Lidé by proto podle něho měli k veřejným sítím přistupovat obezřetně. „Vždy je dobré si uvědomit, zda požadovaný úkon – přístup do bankovnictví, přihlášení na firemní server, zadávání hesel a podobně – musím opravdu provést okamžitě, nebo zda mohu počkat na bezpečnější připojení doma nebo v zaměstnání," doporučil Pinta.

PODEZŘELÝ NÁZEV SÍTĚ

Pomoci vyhnout se potížím může několik základních pravidel. Česká bankovní asociace například doporučuje věnovat pozornost tomu, jak se veřejná síť jmenuje. Například pokud nese jméno Public Plzeň, ale uživatel přitom není v Plzni, je to podezřelé. Jakmile se u veřejné Wi-Fi objeví znak otevřeného zámečku, může komunikaci kdokoliv „odposlouchávat". Užitečné pravidlo je i to, že u neznámých sítí by nemělo být povolováno automatické připojování a pro vyšší bezpečnost je dobré používat VPN, tedy virtuální privátní síť.

Jako návod, jak rozpoznat podvodné útoky, může posloužit Kybertest.cz, který připravila právě Česká bankovní asociace. V něm si každý může vyzkoušet svou zdatnost v kybernetické bezpečnosti.

PRAŽSKÝ deník

Vypadal jako profík, říká okolí falešného zdravotníka

Praha – Policie řeší případ falešného zdravotníka. Zkoumá působení muže, který se staral o pacienty v Praze i v okolí hlavního města. Podle všeho bez toho, že by ho k tomu opravňovalo dosažené vzdělání.

Péči o pacienty zajišťoval mladý muž působící hned na několika pracovištích tak, že nezavdal důvod ke kritice. Dokonce nevzbudil podezření kolegů, kteří neměli ani tušení, že něco není v pořádku.

Podle deníku Právo, který na případ upozornil včetně toho, že zveřejnil jméno Norbert, dotyčný po zjištění zaměstnavatelů dostal třikrát výhazov. Jak v motolské nemocnici v Praze, tak u záchranné služby v Kralupech nad Vltavou, kde předtím v obou případech působil déle než dva roky a v Rudné u společnosti zajišťující zdravotnickou asistenci s přepravou pacientů. Že musel odejít, Deníku potvrdili všichni uvedení zaměstnavatelé.

Jedním z jeho působišť bylo dětské ARO ve Fakultní nemocnici Motol. Její mluvčí Pavlína Danková k tomu Deníku sdělila, že dotyčný zaměstnanec pracoval jako praktická sestra a poskytoval ošetřovatelskou péči, přičemž byl pod odborným dohledem všeobecné sestry.

„Nedošlo k žádnému poškození pacientů. Nezaznamenali jsme ani žádnou stížnost."

Pavlína Danková, mluvčí FN Motol

„Nedošlo k žádnému poškození pacientů a během jeho působení jsme nezaznamenali ani podanou stížnost," řekla Danková.

Že zmiňovaný mladý muž působil jako nesmírně šikovný profesionál, řekla Deníku Petra Homolová z Asociace samaritánů ČR. Komentovala tak jeho působení na výjezdové základně záchranné služby v Kralupech nad Vltavou. Podle Homolové bylo jeho dvouleté působení u zachránců zcela bezproblémové. Ostatně i samotný nástup. „Nebyl žádný důvod k podezření," konstatovala s tím, že zfalšované diplomy působily důvěryhodně: podpořil to údaj, že dotyčný pracuje v Motole. Prověřování přišlo až na základě upozornění z Rudné. **(hol)**

více na prazsky.denik.cz

JIHLAVSKÝ deník

Nejmladší čtyřnásobná dárkyně vlasů je z Jihlavy

JIŘÍ KAŠPÁREK

Je jí teprve devět let, ale pomáhá lidem s rakovinou, trpícím vypadáváním vlasů. Róza Kloknerová z Jihlavy je nejmladší čtyřnásobnou dárkyní vlasů v republice. Dívka je zároveň dětskou rekordmankou. Poprvé vlasy darovala už ve čtyřech letech. Díky svému neutuchajícímu dárcovství se ve středu v Pelhřimově zároveň zapsala do České knihy rekordů.

Róza jde ve šlépějích rodičů. „S manželem chodíme darovat krev, byli jsme i v registru dárců kostní dřeně. A dceři vlasy rostou extrémně rychle. Průměr je jeden centimetr za měsíc. Přišlo nám proto jako škoda je vyhodit. Doma jsme zjistili, že je můžeme darovat i v jihlavském kadeřnictví. Původně jsme ani nevěděli, že se nějaký rekord podaří," popsala začátky maminka Rózy Martina.

V Česku je Róza jediná, kdo pomáhá v tak mladém věku a v takovém rozsahu. Může dokonce jít i o evropský unikát. „S něčím takovým jsem se ještě nesetkal. Nemáme ani žádnou informaci, že by byl takový dárce v Evropě. Ale vyhlásili jsme to jako český rekord, protože nemáme sílu prověřit všechny státy," řekl Deníku Miroslav Marek z Agentury Dobrý den, která rekordy zaštiťuje.

Dívka vlasy poprvé darovala v roce 2017. Poté si je pro nemocné nechala ostříhat v letech 2019 a 2020. Vlasy pokaždé měřily od pětadvaceti do třiceti centimetrů. Rózu Kloknerovou pravidelně stříhá kadeřnice Šárka Křížová z Jihlavy. „Je speciální střihat rekordmanku, to nebývá každý den. Navíc v kadeřnictví bývám se zákazníkemi sama. Takže to bylo jiné i v počtu lidí okolo," přibližila.

Křížová zároveň ve středu darovala sto sedm culíků nadační Gracie, která dárcovství vlasů podporuje. „Spolupracujeme tři roky od doby, kdy mě oslovili. Každým rokem se podaří dát vlásků víc a víc. Hlavní podmínkou darování je délka, která by měla dosahovat třiceti centimetrů. Zákaznice už jsou na to u mě zvyklé. Když si chtějí vlasy zkrátit, jdou do toho s tím, že je darují," popsala kadeřnice.

132. Křišťálová Lupa 2022 zná vítěze. Osobností roku je Jan Bednář, Projektem roku Zbraneproukrajinu.cz

Online ● focus-age.cz (Podnikání / Marketing / PR) ● 24. 11. 2022, 3:49

Vydavatel: **Focus agency s.r.o. (cz-26212722)**

Dosah: 1 873 ● GRP: 0.02 ● OTS: 0.00 ● AVE: 7395.83 Kč

Odkaz: https://www.focus-age.cz/m-journal/aktuality/kristalova-lupa-2022-zna-viteze--osobnosti-roku-je-jan-bednar--projektem-roku-zbraneproukrajinu-cz__s288x16897.html

FOCUS A

ATA ČLÁNKŮ ZVOLTE OBDOBÍ HLEDAT VÝRAZ vyhledat..

Všechny články

Křišťálová Lupa 2022 zná vítěze. Osobností roku je Jan Bednář, Projektem roku Zbraneproukrajinu.cz

24. 11. 2022 | redakce

Osobností roku v 17. ročníku ankety Křišťálová Lupa – Cena českého Internetu se stává zakladatel start-upu Shipmonk Jan Bednář, titul Projekt roku získává server Zbraneproukrajinu.cz. Cenu popularity si odnáší Opravdové zločiny.

Letošní ročník ankety Křišťálová Lupa – Cena českého internetu je u konce. V Divadle pod Palmovkou byly ve čtvrtek 24. listopadu večer slavnostně vyhlášeny a rozdány ceny vítězům ve všech kategoriích. Rozhodly o nich svými hlasy odborná porota a internetová veřejnost. Do hlasování se letos zapojilo více než sto dvacet tisíc hlasujících. Anketu pořádá server Lupa.cz.

organizace, instituce a dlouhodobé aktivity pro podporu Ukrajiny, stejně jako individuální a jednorázová pomoc.

2. Donio - Dárcovská platforma, na které může každý snadno vytvořit sbírku.
3. (3. – 4.) Hlídač státu - Nástroj, který nabízí kontrolní nástroje u vybraných služeb státu.
4. (3. – 4.) Aplikace Záchranka - Aplikace na zavolání záchranné nebo horské služby, která překonala 1 milion stažení.
5. Ověřovna! - Projekt Českého rozhlasu, který se snaží vysvětlovat a ověřovat nepravdivé informace nebo překroucená fakta.
6. Spolek NELEŽ - Apelace na inzerenty, aby svou reklamou nefinancovali dezinformační weby. Cílem je omezit šíření dezinformací v online prostoru.
7. Beztrestu.cz - Server proti zlehčování sexualizovaného a domácího násilí.
8. Patron dětí - Charitativní projekt, který se snaží pomáhat zdravotně a sociálně znevýhodněným dětem a jejich rodinám z celé České republiky.
9. (9. – 11.) Programy do voleb - Neziskový projekt nabízející přehledné informace o stranách, kandidátech a volebních programech.
10. (9. – 11.) Movapp - Ukrajinsko-český slovník.
11. (9. – 11.) Kybertest - Interaktivní vzdělávací kybertest České bankovní asociace.

Štítky dokumentu: Tipy na akce

133. Křišťálová Lupa 2022: Osobností roku je Jan Bednář z Shipmonku, projektem Zbraně pro Ukrajinu

Online ● lupa.cz (IT / Technologie) ● 24. 11. 2022, 21:00

Vydavatel: **Internet Info, s.r.o. (cz-25648071)**

Dosah: 27 681 ● GRP: 0.31 ● OTS: 0.00 ● AVE: 22778.02 Kč

Odkaz: https://www.lupa.cz/clanky/kristalova-lupa-2022-osobnosti-roku-je-jan-bednar-z-shipmonku-projektem-zbrane-pro-ukrajinu/

Veřejně prospěšná služba – cena České televize

1. Stojíme za Ukrajinou a Pomáhej Ukrajině - Odkazy na pomáhající organizace, instituce a dlouhodobé aktivity pro podporu Ukrajiny, stejně jako individuální a jednorázová pomoc.
2. Donio - Dárcovská platforma, na které může každý snadno vytvořit sbírku.
3. (3. – 4.) Hlídač státu - Nástroj, který nabízí kontrolní nástroje u vybraných služeb státu.
4. (3. – 4.) Aplikace Záchranka - Aplikace na zavolání záchranné nebo horské služby, která překonala 1 milion stažení.
5. Ověřovna! - Projekt Českého rozhlasu, který se snaží vysvětlovat a ověřovat nepravdivé informace nebo překroucená fakta.
6. Spolek NELEŽ - Apelace na inzerenty, aby svou reklamou nefinancovali dezinformační weby. Cílem je omezit šíření dezinformací v online prostoru.
7. Beztrestu.cz - Server proti zlehčování sexualizovaného a domácího násilí.
8. Patron dětí - Charitativní projekt, který se snaží pomáhat zdravotně a sociálně znevýhodněným dětem a jejich rodinám z celé České republiky.
9. (9. – 11.) Programy do voleb - Neziskový projekt nabízející přehledné informace o stranách, kandidátech a volebních programech.
10. (9. – 11.) Movapp - Ukrajinsko-český slovník.
11. (9. – 11.) Kybertest - Interaktivní vzdělávací kybertest České bankovní asociace.

134. Podcastem roku jsou Opravdové zločiny, nejlepší videa dělají Kluci z Prahy. Známe výsledky Křišťálové lupy

Online ● refresher.cz (Společenské) ● 24. 11. 2022, 21:19

Vydavatel: **REFRESHER Media CZ, s.r.o. (cz-06090389)** ● Autor: **Adam Smeták**

Dosah: 43 359 ● GRP: 0.48 ● OTS: 0.00 ● AVE: 30471.11 Kč ● Interakcí: 43

Odkaz: https://refresher.cz/125759-Podcastem-roku-jsou-Opravdove-zlociny-nejlepsi-videa-delaji-Kluci-z-Prahy-Zname-vysledky-Kristalove-lupy

ČESKO 0 Adam Smeták dnes 24. 11. 2022 21:19 Čas čtení: 2:13

Podcastem roku jsou Opravdové zločiny, nejlepší videa dělají Kluci z Prahy. Známe výsledky Křišťálové lupy

Předávání cen Křišťálová lupa 2022 je za námi. Odborná porota a veřejnost v hlasování vybrali nejlepší projekty českého internetu.

Ve čtvrtek večer proběhlo předávání cen ankety Křišťálová Lupa 2022, kterou pořádá server Lupa.cz. Sošky si odnášejí nejoblíbenější a nejzajímavější projekty, služby a osobnosti českého internetu.

1. Zbraneproukrajinu.cz
2. Diskuse Seznamu
3. Productboard.com
4. – 8. Rohlík.cz
4. – 8. Česko.digital
4. – 8. Čeští elfové
4. – 8. CzechFounders
4. – 8. Prodej Avastu
9. Pickey
10. Voyo.cz

Veřejně prospěšná služba – cena České televize

1. Stojíme za Ukrajinou a Pomáhej Ukrajině
2. Donio
3. – 4. Hlídač státu
3. – 4. Aplikace Záchranka
5. Ověřovna!
6. Spolek NELEŽ
7. Beztrestu.cz
8. Patron dětí
9. – 11. Programy do voleb
9. – 11. Movapp
9. – 11. Kybertest

Globální projekty českých tvůrců

1. Windy.com
2. Livesport.cz
3. – 4. Productboard.com
3. – 4. Průša3D.cz
5. ShipMonk
6. – 8. CDN77.com
6. – 8. Rohlík.cz
6. – 8. Rossum.ai

135. Křišťálová Lupa 2022: Ceny jsou rozdány. Kdo vyhrál?

Online ● runwayonline.cz (Životní styl / Móda) ● 25. 11. 2022, 19:34

Vydavatel: **Jana Fikotová (cz-86577336)** ● Autor: **Kamila Šimková** ● Rubrika: **aktuálně**

Dosah: 15 088 ● GRP: 0.17 ● OTS: 0.00 ● AVE: 17847.13 Kč

Odkaz: https://runwayonline.cz/tema/kristalova-lupa-2022-ceny-jsou-rozdany-kdo-vyhral/

Avokádo: skvělé k jídlu i na pleť

Čím si připijeme na nový rok? Naučte se míchat koktejly

aktuálně, kultura, téma, TOP, TOP téma, zábava

Křišťálová Lupa 2022: Ceny jsou rozdány. Kdo vyhrál?

Kamila Šimková 25 listopadu, 2022

foto: Lupa.cz

Letošní ročník ankety Křišťálová Lupa – Cena českého internetu vyhlásil v Divadle pod Palmovkou své vítěze. O nich rozhodla svými hlasy odborná porota i internetová veřejnost. Do hlasování se letos zapojilo více než sto dvacet tisíc hlasujících.

Osobností roku v 17. ročníku ankety Křišťálová Lupa – Cena českého Internetu se stal zakladatel start-upu Shipmonk Jan Bednář, titul Projekt roku získal server Zbraneproukrajinu.cz., Cenu popularity a Nejlepší podcast si odnáší podcast Opravdové zločiny.

Anketa Křišťálová Lupa 2022 – Cena českého Internetu pravidelně oceňuje nejoblíbenější a nejzajímavější projekty a služby českého Internetu. Letos proběhl již 17. ročník této nejvýznamnější internetové ankety, kterou pořádá server Lupa.cz. Vedle této tradiční ankety byl uspořádán rovněž 17. ročník odborné konference Czech Internet Forum 2022, mapující aktuální stav českého Internetu z mnoha úhlů pohledu.

Odborná porota je tradičně složená z významných osobností podnikatelského, mediálního a internetového světa. Svým hodnocením určuje pořadí v uvedených kategoriích.

Veřejně prospěšná služba – cena České televize

1. Stojíme za Ukrajinou a Pomáhej Ukrajině
2. Donio
3. – 4. Hlídač státu
3. – 4. Aplikace Záchranka
5. Ověřovna!
6. Spolek NELEŽ
7. Beztrestu.cz
8. Patron dětí
9. – 11. Programy do voleb
9. – 11. Movapp
9. – 11. Kybertest

136. Nikdy nevíš, kdo se dívá. Veřejná wi-fi síť je vstupenkou pro hackery

Online ● denik.cz (Zprávy / Politika) ● 25. 11. 2022, 19:40

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)** ● Autor: **Vilém Janouš**

Dosah: 529 030 ● GRP: 5.88 ● OTS: 0.06 ● AVE: 58042.39 Kč ● Interakcí: 52

Odkaz: https://www.denik.cz/krimi/verejna-wifi-nebezpeci-20231123.html

Nikdy nevíš, kdo se dívá. Veřejná wi-fi síť je vstupenkou pro hackery

DNES 19:40

Vilém Janouš
Editor
Napište mi

Pan Jaroslav se před nedávnem přihlásil do veřejné wi-fi sítě. Přes ni se proklikal až na stránku, která vyhlížela jako reálný e-shop. Objednal si zboží a rozhodl se rovnou zaplatit. Stránka ho následně přesměrovala na platební bránu, v níž vyplnil všechny požadované údaje a zaplatil. Že šlo o podvod, poznal až ve chvíli, kdy mu hackeři ukradli z karty peníze až do jejího limitu. Jak upozorňují odborníci, ve veřejné wi-fi síti nikdo neví, kdo do jeho soukromí právě nahlíží.

Češi nejsou na svoje soukromí zrovna hákliví. Veřejné wi-fi sítě podle průzkumu využívají asi tři čtvrtiny lidí, třetina dotázaných dokonce k internetovému bankovnictví. Ilustrační snímek | *Foto: Shutterstock*

„Nikdy nevíte, kdo veřejnou wi-fi síť skutečně provozuje a jaké má úmysly. U přistupování na webové stránky, které nepoužívají šifrování, může dojít velmi snadno k odchycení celé komunikace, tedy všeho, co si na dané webové stránce uživatel prohlíží, odesílá nebo třeba jaké vyplňuje osobní údaje," upozornil Jan Pinta ze společnosti Thein Security, které se zabývá kybernetickou bezpečností.

Mobily nebo laptopy přitom uchovávají o jejich majiteli mnoho citlivých informací, ať jsou to fotky, kontakty, hesla nebo přístupy do online bankovnictví. To všechno jsou informace, které **podvodníky** zajímají.

Hackeři masivně útočí na e-maily. Čechy se snaží nachytat na faktury z dovolené

PŘEČÍST ČLÁNEK ›

Jak se zdá, Češi ovšem nejsou na svoje soukromí na internetu zrovna hákliví. Průzkum společnosti Anect ukázal, že veřejné sítě využívají tři čtvrtiny Čechů. Dvě třetiny z nich je používají k e-mailové komunikaci a jedna třetina

dotázaných dokonce k internetovému bankovnictví.

„Pro útočníky je přitom velmi snadné, aby buďto ovládli nechráněnou veřejnou wi-fi například v hotelu nebo, což je pro ně úplně nejjednodušší varianta, aby postavili svoji vlastní wi-fi například s názvem některé z oblíbených restaurací. Návštěvníci si potom neuvědomují, že pokud nepoužívají automaticky všude ochranu pomocí šifrování, první část jejich komunikace, která směřuje na tuto podvodnou wi-fi, je pro útočníka kompletně čitelná," uvedl expert na kybernetickou bezpečnost ze společnosti Anect Ivan Svoboda.

Nepozorní jsou i odborníci

Lehkovážně k veřejným wi-fi sítím nepřistupuje jen běžná laická veřejnost, ale někdy i v oboru kovaní odborníci. To před několika lety ukázal experiment společnosti Avast. Na kongresu věnovaném mobilní komunikaci v Barceloně vytvořila kolem registračního stánku několik falešných veřejných wi-fi sítí s názvy, jako je například „Airport_Free_Wifi_AENA" nebo „Starbucks". Jen během čtyř hodin se do těchto sítí přihlásilo dva tisíce lidí. Společnost zároveň zjistila, že ve více než 60 procentech případů bylo možné zjistit identitu uživatele.

Jaké komunikační aplikace využívat? NÚKIB nejvíce doporučuje Threema a Signal

PŘEČÍST ČLÁNEK ›

Právě na to upozornil také Jan Pinta z Thein Security. Falešné veřejné sítě se často mohou vydávat za na první pohled známé sítě, přičemž se jedná pouze o další podvod a nalákání oběti. „Na veřejných sítích se také často objevuje snaha o **vylákání údajů k platební kartě** nebo k instalaci softwaru, který následně komunikaci odposlouchává," doplnil expert.

Lidé by proto podle něho měli k veřejným sítím přistupovat obezřetně. „Vždy je dobré si uvědomit, zda požadovaný úkon – přístup do bankovnictví, přihlášení na firemní server, zadávání hesel a podobně – musím opravdu provést okamžitě

na firemní server, zadávání hesel a podobně – musím opravdu provést okamžitě, nebo zda mohu počkat na bezpečnější připojení doma nebo v zaměstnání," doporučil Pinta.

Základní pravidla

Zásadní problém s veřejnými sítěmi ovšem vyvstává v době dovolených, kdy mnoho lidí na takových sítích vyřizuje svoje pracovní e-maily. „Pokud nepoužívají kontinuální a spolehlivé šifrování, může se potenciální útočník dostat k obsahu dané komunikace, k jejich přístupovým heslům, a nakonec i do interní firemní sítě," varoval Svoboda. A to může ohrozit chod celé firmy.

Pomoci vyhnout se těmto potížím může několik základních pravidel. Česká bankovní asociace například doporučuje věnovat pozornost tomu, jak se veřejná síť jmenuje. Například pokud nese jméno Public Plzeň, ale uživatel přitom není v Plzni, je to podezřelé. Jakmile se u veřejné wi-fi objeví znak otevřeného zámečku, může komunikaci kdokoliv „odposlouchávat".

Gangy na síti. Hackeři útočí častěji a jsou rychlejší, nepodceňte volbu hesla

PŘEČÍST ČLÁNEK ›

Užitečné pravidlo je i to, že u neznámých sítí by nemělo být povolováno automatické připojování a pro vyšší bezpečnost je dobré používat VPN, tedy virtuální privátní síť. Pokud přesto musí uživatel použít veřejnou síť, rozhodně by neměl nikam zadávat citlivé údaje.

Jako užitečný návod, jak rozpoznat podvodné útoky, může posloužit **Kybertest.cz**, který připravila právě Česká bankovní asociace. V něm si každý může vyzkoušet svou zdatnost v kybernetické bezpečnosti.

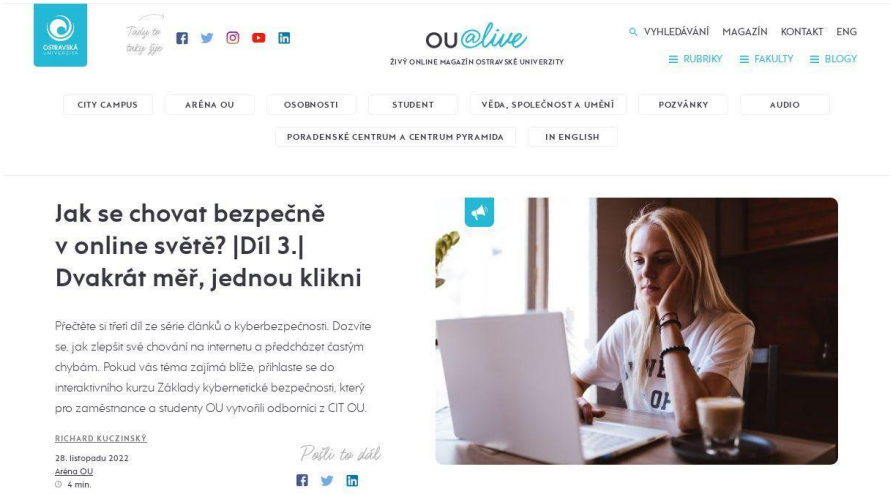
137. Jak se chovat bezpečně v online světě? |Díl 3.| Dvakrát měř, jednou klikni

Online ● alive.osu.cz (Jiné) ● 28. 11. 2022, 8:36

Autor: **Richard Kuczinský** ● Rubrika: **Aréna OU**

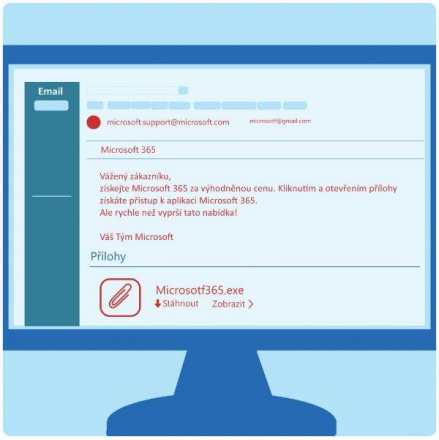
Dosah: 363 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 3049.80 Kč

Odkaz: https://alive.osu.cz/jak-se-chovat-bezpecne-v-online-svete-dil-3-dvakrat-mer-jednou-klikni/



Radek je šikovný student magisterského programu, který doučuje a školí lidi ze svého okolí. To zahrnuje práci se spoustou osobních dat svých žáků. Do e-mailu Radkovi přišla zpráva, která odkazuje na přihlašovací okno systému, kde eviduje své žáky, včetně jejich studia. Odkaz byl doplněný zprávou, že pokud se Radek přihlásí přes zaslaný odkaz ještě ten daný den, dostane zdarma přístup ke dvěma novým modulům systému, které jeho vzdělávání posunou o další úroveň výše.

Obsah zprávy zněl velmi lákavě a pokud by Radek své údaje vyplnil a odeslal, putovaly by přímo do rukou útočníka. Tento příběh je postavený na reálné zkušenosti mnoha uživatelů, jedná se totiž o ukázkový phishing, kdy útočník rozesílá hromadně velké množství podvodných e-mailů a snaží se tak sbírat přihlašovací údaje. Ty pak může libovolně zneužít.



Bezpečnostní útok nazývaný phising je jednou z technik sociálního inženýrství, které pro své cíle využívá velmi citlivou metodu – psychologickou manipulaci, a to skrze přirozené lidské slabosti, tedy například zvědavost, strach či nepozornost. Skrze tento typ manipulace dokáže útočník svou oběť dokonale oklamat. Ta se může následně dopustit bezpečnostní chyby a poskytnout tak útočníkovi informace v podobě citlivých údajů a přístupových práv, nebo rovnou peněžních částek.

Jak se takové chyby vyvarovat?

1. **Důvěřuj, ale prověřuj.** Zapojte kritické myšlení – proč by vám na internetu dával někdo něco zdarma? Jak již navíc víte z předchozích dílů tohoto seriálu, ne každý e-mail musí být skutečně od toho odesílatele, od jakého se zdá, že je.
2. **Útok je skryt v detailu.** Soustřeďte se na gramatiku a pravopis zprávy – podivné formulace a chyby by každého uživatele měly ihned zalarmovat.
3. **Dvakrát měř, jednou klikni.** Pořádně si prohlédněte URL odkaz (někdy může jít jen o prohozená písmenka v adresním řádku), ale i celkovou grafickou podobu stránky. I drobné nuance mohou být předzvěstí nekalosti. Navíc platí, že heslo nikdy nezadáme přes odkaz, který nám někdo zašle.

Vyzkoušejte si, jaké to může být v podobných situacích, jakou zažil Radek. Poznáte phishing a další zákeřné metody? Odhalíte je dostatečně brzy? Otestovat se můžete na webu KYBERTEST, v testu od Google nebo ve slovenské verzi podobného testu na webu CSIRT.SK.

Technik sociálního inženýrství je celá řada – do emailu vám může přijít výzva k zaplacení vyšších i nižších částek, a to jak tvářící se jako korespondence od známých institucí a organizací, tak od vašich známých či kolegů.

Útoky se však netýkají jen emailů. Zvýšit svou pozornost je třeba u jakéhokoliv typu přihlašování, je důležité se soustředit na gramatiku textu a grafické zpracování stránky. K útoku může dojít také prostřednictvím SMS zprávy nebo podvodného telefonátu. Leckterý uživatel si neuvědomí, že takový útok může mít podobu doručovací SMS od dodávky jídla nebo hovoru s osobou vydávající se za bankovního poradce.

Jak je důležité v takových případech postupovat?

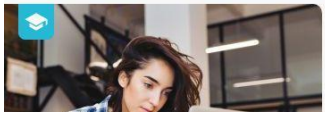
Nikdy nikomu nesdělujte své heslo a PIN (písemně ani telefonicky) a nepřihlašujte se prostřednictvím odkazů, které vám někdo zašle v emailu. Vždy zachovávejte chladnou hlavu – přemýšlejte nad tím, proč by po vás mohl někdo něco podobného chtít a v neposlední řadě se nenechte ovlivnit nátlakem („Když se nezaregistrujete do 15 minut, přijdete o všechny výhody!"). Ideální je se permanentně kriticky zamýšlet nad tím, na co a proč na internetu klikáte a všímat si podezřele vypadajících aspektů stránek a mailů.

Vhodným postupem je vždy tuto odhalenou podvodnou činnost nahlásit. Pokud se vám zdají požadavky, které vám dorazily na pracovní či školní email, podezřelé nebo v případě, že phishingu podlehnete, vše obratem nahlaste na security@helpdesk.osu.cz.

Pokud byste odhalili podvodný hovor, zaznamenejte si číslo, ze kterého vám bylo voláno, čas a jaké údaje chtěl útočník vědět. S těmito informacemi je vhodné se poté obrátit na policii, mohou totiž výrazně pomoci při dopadení pachatele.

Chcete se dozvědět více o tom, jak se na internetu chovat bezpečně? Zapojte se do online kurzu nazvaného *Základy kybernetické bezpečnosti*, který vytvořili odborníci z Centra informačních technologií OU pro zaměstnance a studenty univerzity. Na konkrétních případech si projdete nejčastější chyby, kterých se uživatelé dopouští a naučíte se, jak jim předcházet a účinně se bránit. Kurz najdete na tomto odkaze.

MOHLO BY VÁS ZAJÍMAT



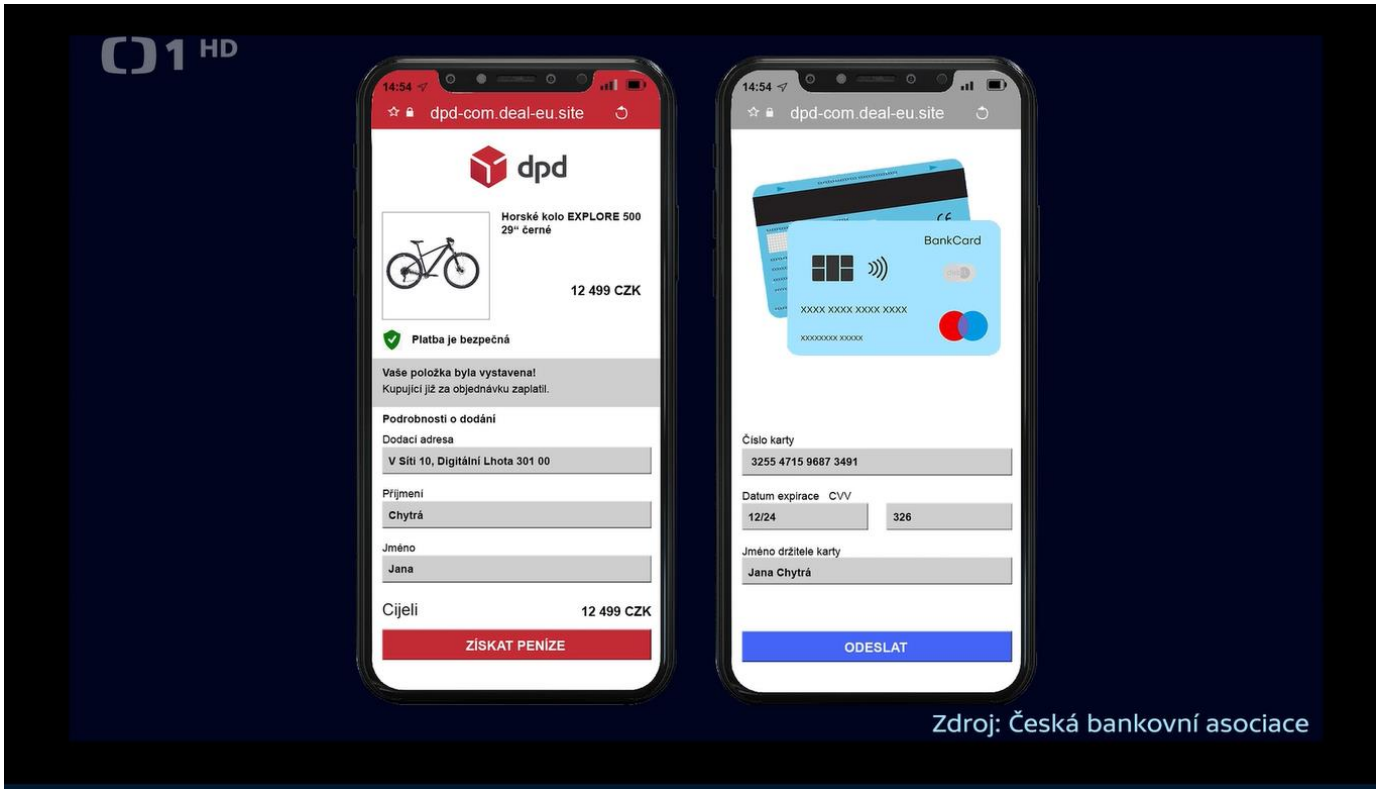
138. Studio 6: 29. listopad

Televize ● Studio 6 (ČT1) ● 29. 11. 2022, 5:59

Vydavatel: **ČESKÁ TELEVIZE (cz-00027383)**

Dosah: 79 759 ● GRP: 0.89 ● OTS: 0.01 ● AVE: 18839474.59 Kč

Odkaz: https://www.ceskatelevize.cz/porady/1096902795-studio-6/222411010101129/



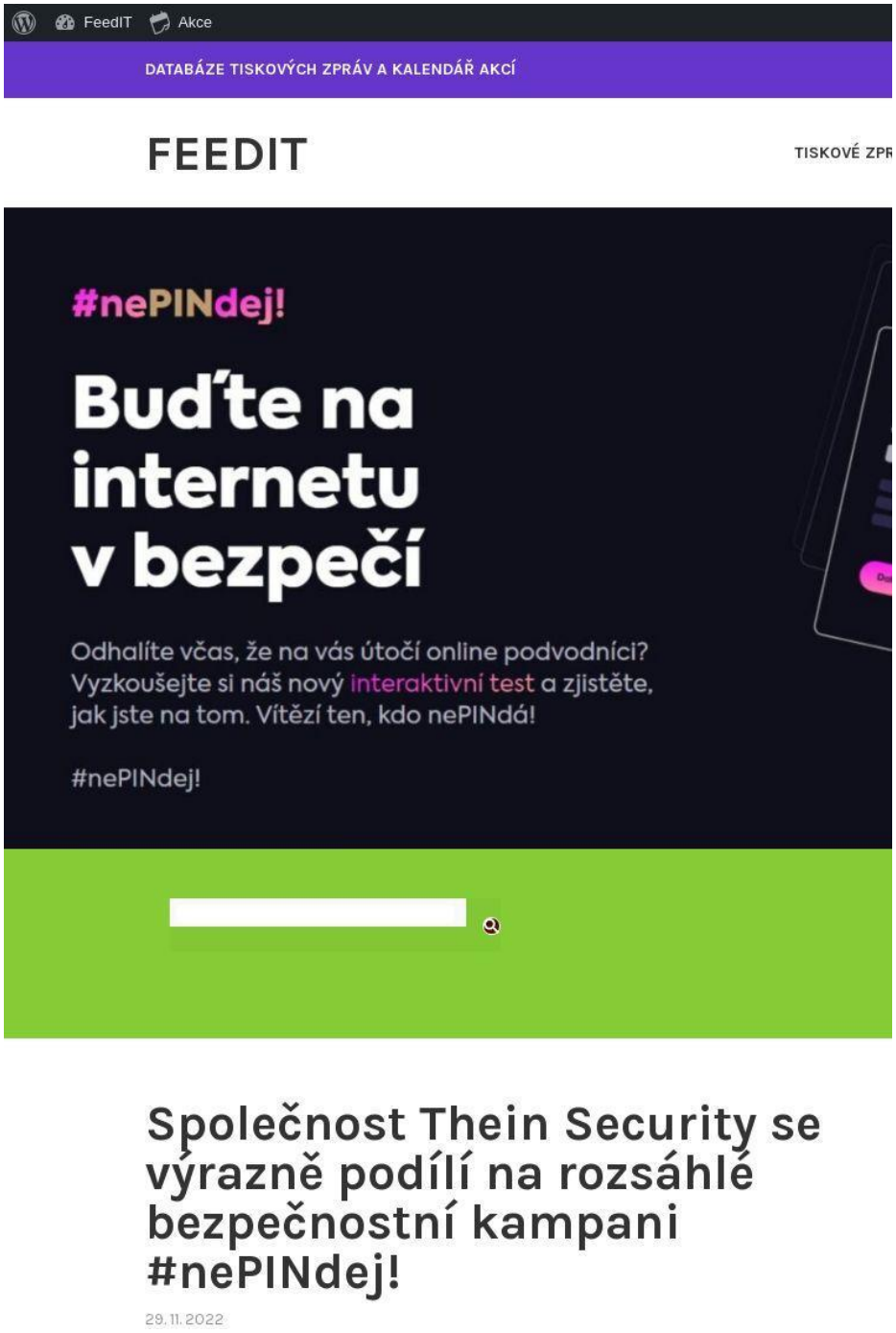
139.Společnost Thein Security se výrazně podílí na rozsáhlé bezpečnostní kampani #nePINdej!

Online ● feedit.cz (Podnikání / Marketing / PR) ● 29. 11. 2022, 9:41

Vydavatel: **FEED IT CZ s.r.o. (cz-09695931)** ● Rubrika: **Tisková zpráva**

Dosah: 2 047 ● GRP: 0.02 ● OTS: 0.00 ● AVE: 7718.83 Kč

Odkaz: https://feedit.cz/2022/11/29/spolecnost-thein-security-se-vyrazne-podili-na-rozsahle-bezpecnostni-kampani-nepindej/



29. listopadu 2022, Praha – Společnost Thein Security poskytující komplexní služby spojené s ochranou firem v kyberprostoru úspěšně podporuje vzdělávací kampaň #nePINdej! ve spolupráci s Českou bankovní asociací. Kampaň, jejíž hlavním cílem je edukovat širokou veřejnost a upozorňovat na problémy finančních scamů, běží od začátku září a jejím klíčovým prvkem je interaktivní **kybertest**, na jehož přípravě se bezpečnostní odborníci Thein Security výrazně podíleli.

V současné době počet kybernetických útoků, a především těch zvaných DDoS, v Čechách nekontrolovatelně narůstá. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) jich v letos říjnu evidoval devatenáct, což je o jeden méně než v rekordním dubnu. Není tak pochyb, že ve firmách i domácnostech již nelze brát kybernetickou bezpečnost na lehkou váhu, protože terčem může být kdokoliv. Nebezpečí dnes číhá bohužel téměř všude, včetně veřejných nezabezpečených wifi sítích, které uživatelé často bezmyšlenkovitě používají a sdílejí tak část svého digitálního soukromí i důležité přihlašovací údaje. Vytvořit falešnou veřejnou wifi síť, která na první pohled působí důvěryhodně a vylákat následně z uživatelů údaje je přitom pro útočníky jednou z nejsnazších cest.

Rozsáhlá celostátní vzdělávací kampaň pod záštitou České bankovní asociace, na které právě spolupracuje mimo jiné i NÚKIB, sklízí od svého spuštění na začátku září nevídaný úspěch. Kyberbezpečnostní experti Thein Security přispěli svým know-how a pomohli z velké části realizovat klíčový prvek kampaně, a to interaktivní vzdělávací kybertest. Ten zábavnou formou testuje znalosti veřejnosti o nejčastějších kybernetických podvodech a upozorňuje na to, jak je rozpoznat od ověřených požadavků.

Z dat z výzkumu realizovaným ČBA vyplývá, že více než polovina (58 %) Čechů se někdy setkala s nějakou formou hackerského útoku, téměř třetina (32 %) zná pak ve svém blízkém okolí někoho, kdo se stal obětí dokončeného útoku. Přitom nejčastěji se lidé setkávají s útoky přes e-mailové zprávy a sociální sítě. Nejběžněji útočníci cílí na poskytnutí přihlašovacích údajů.

"Kampaň #nePINdej! je v podstatě ztělesněním toho, o co nám v Thein Security jde. Zvyšovat bezpečnostní povědomí veřejnosti, šířit mezi firmy informace o tom, co se může stát a představit ty nejběžnější praktiky sociálního inženýrství. Bezpečnostní povědomí se ve firmách i společnosti musí budovat. Jsme pyšní na to, že jsme součástí tak rozsáhlé kampaně v našem oboru a mohli jsme našimi znalostmi přispět k úspěšné realizaci," nechává se slyšet **Irena Hýsková**, ředitelka společnosti Thein Security, která se mimo jiné soustředí právě na

zabezpečení lidského faktoru formou školení kybernetické bezpečnosti či simulací phishingových útoků

"Phishingové útoky jsou v dnešní době čím dál sofistikovanější a úspěšnost útočníků je bohužel velmi vysoká. Jsou agresivnější, chytřejší a jednotlivé kroky mají předem dobře naplánované. Oběťmi dnes zdaleka nejsou jen senioři, ale kterýkoliv uživatel internetu. Kybertest je výborným vstupním testem na ověření znalostí každého z nás," dodává **Jan Pinta**, kyberbezpečnostní expert Thein Security. Součástí testu, který rozhodně nemá za cíl lidi nachytat, je navíc také poučné desatero bezpečného chování na internetu, na jehož tvorbě se Jan Pinta podílel.

Kampaň zaměřující se na edukaci všech věkových kategorií, od školáků až po seniory, v popředí s **kybertestem** poběží do konce roku a vidět bude mimo jiné třeba i na bankomatech po celém Česku.

O Thein Security

Thein Security, součást skupiny Thein, zastřešuje veškeré její aktivity v oblasti kybernetické bezpečnosti. Thein Security nabízí komplexní služby spojené s ochranou firem v kyberprostoru, včetně prevence úniku citlivých dat, obrany proti sofistikovaným útokům, detekce neznámého malware nebo aktivní ochrany proti DDoS útokům. Jednou z hlavních specializací firmy je vlastní bezpečnostní středisko SOC (Security Operations Center), které je poskytováno těm zákazníkům, kteří se chtějí soustředit na své podnikání, ale současně vyžadují prvotřídní dohled nad ochranou svých dat v kyberprostoru.

140. Češi hazardují s penězi. Lákavá nabídka na internetu může přijít pěkně draho

Online ● jicinsky.denik.cz (Regionální zprávy) ● 4. 12. 2022, 10:15

Vydavatel: **VLTAVA LABE MEDIA a.s. (cz-01440578)** ● Autor: **Vilém Janouš**

Dosah: 965 223 ● GRP: 10.72 ● OTS: 0.11 ● AVE: 852228.93 Kč

Odkaz: https://jicinsky.denik.cz/zpravy-z-ceska/nabidky-na-internetu-podvod.html

Češi hazardují s penězi. Lákavá nabídka na internetu může přijít pěkně draho

DNES 10:15

Vilém Janouš
Editor
Napište mi

Ta cena byla neodolatelná. Není proto divu, že firma z Náchodska podlehla vábení e-shopu, na němž si koupila čtyři notebooky. Jenže ta výhodnost platila jen do zaplacení zálohové faktury několik desítek tisíc korun. Pak se po e-shopu slehla zem. Firma se stala obětí podvodného internetového obchodu.

Podvodné e-shopy přitom využívají nejen totožný vzhled, jakým disponují ty legitimní, ale také oficiální loga společností nebo i stejný název internetové domény | *Foto: Shutterstock*

„Podvodníci v tomto případě často využívají anonymní povahu internetu za účelem okradení naivních, nepozorných a nic netušících nakupujících. Pomocí nejnovějších technologií jsou schopni vytvořit falešné internetové stránky, které jsou téměř k nerozeznání od těch legitimních," uvedla specialistka kybernetické bezpečnosti Českých drah Nicol Moravcová.

Kupte si nerozbalené dárky, láká web vypadající jako Česká pošta. Je to podvod

PŘEČÍST ČLÁNEK ›

Podvodné e-shopy přitom využívají nejen totožný vzhled, jakým disponují ty legitimní, ale také oficiální loga společností nebo i stejný název internetové domény. Přesto se vyznačují určitými znaky, které by měly potenciální zákazníky varovat, že něco není v pořádku. Zejména nabízejí luxusní zboží a oblíbené světoznámé značky za nezvykle nízké ceny. „Po objednání zboží nakupující buď obdrží položku, za kterou si zaplatil, nicméně bude falešná, anebo položku neobdrží vůbec," přiblížila Moravcová.

Podezřelý může být i způsob platby. Podvodné internetové obchody požadují

platbu pomocí peněžní poukázky, předem nabité platební karty nebo pouze pomocí okamžitého bankovního převodu.

Množí se telefonáty od falešných bankéřů. Lidé mohou přijít o statisíce

PŘEČÍST ČLÁNEK ›

Potenciálním zákazníkům by tedy měla naskočit červená varovná kontrolka, jestliže takový obchod inzeruje produkty za neobvykle nízkou cenu nebo požaduje okamžitou platbu před odesláním zboží. „Varovným znakem může být i to, že internetový obchod neposkytuje dostatečné informace o soukromí, podmínkách používání, řešení sporů, zpracování osobních údajů nebo nemá uvedeny kompletní kontaktní údaje," přiblížila expertka.

Samotné České dráhy mají s podvodnými e-shopy svoje zkušenosti. Některé přeprodávají jejich jízdenky bez zprostředkovatelské smlouvy, často se změněnými údaji a se změněnou cenou. Dopravce varuje, že takové jízdenky neuznává. Jedná se hlavně o jízdenky na mezinárodní trasy.

Škodná v mobilu

Obezřetnost je na místě i před podvodnými aplikacemi. V některých případech se může jednat až o desítky tisíc napadených uživatelů, kterým zloději pomocí těchto programů natropí škody až za stovky milionů korun.

„Jedná se o aplikace, které po stažení například kontrolují polohu zařízení uživatele, telefonní číslo a tak dále, aby zjistily, v jakém jazyce půjde podvod uskutečnit. Po otevření aplikace je uživatel požádán o zadání telefonního čísla, případně e-mailové adresy a dalších citlivých údajů," přiblížil mluvčí společnosti ČEZ Martin Schreier.

Kupte si nerozbalené dárky, láká web vypadající

Kupte si nerozbalené dárky, taká web vypadající jako Česká pošta. Je to podvod

PŘEČÍST ČLÁNEK ›

Útočníci zpravidla zneužívají aplikace a služby, které lidé používají ve volném čase, jako jsou například hry. Jakmile se takto dostanou například k heslům, okamžitě je zneužijí třeba při přihlašování do internetového bankovnictví.

Existují určité znaky, které pomůžou podvodnou aplikaci odhalit. Prvním vodítkem může být třeba chybějící diakritika nebo zvláštní čeština, kterou je dotazník formulován. Důvodem k pochybnostem může být i znění webové adresy. Ta sice může obsahovat název konkrétní banky, ale doménu už má jinou.

„Základním pravidlem ovšem je, že do internetového bankovnictví se člověk přihlašuje jen proklikem ze skutečné domovské stránky banky, ne přes odkaz v mailu nebo sms. Skutečná banka, energetika nebo e-shopy po klientech nikdy nechtějí žádné přístupy do bankovnictví, jeho zákaznických účtů nebo jiné citlivé údaje, které se podvodníci snaží od klientů dostat," upřesnil Schreier.

SMS nebo e-mail. Zprávy od hackerů umí nepozorné připravit o desetitisíce korun

PŘEČÍST ČLÁNEK ›

Škodám, které mohou podvodné aplikace způsobit, lze předejít. Především by lidé měli takové aplikace stahovat z důvěryhodných zdrojů, jako jsou například platformy Google Play nebo App Store. Ještě před jejich stažením by si měli přečíst výběr z recenzí a hodnocení. „Dobrým indikátorem je třeba počet lidí, kteří si už stáhli aplikaci. Čím vyšší počet stažení, tím je aplikace důvěryhodnější," doplnil Schreier.

Nový seriál Deníku: Digitální podvody. *Zdroj: Deník*

V poslední době začínají samy firmy přijímat opatření, kterými před škodlivým softwarem chrání sebe i své zaměstnance. Třeba právě ČEZ loni spustil provoz vlastního bezpečnostního dohledového centra. Systém zachytil asi dvacet tisíc útoků.

Jako užitečný návod, jak rozpoznat podvodné útoky, může posloužit Kybertest.cz, který připravila Česká bankovní asociace. V něm si každý může vyzkoušet svou zdatnost v kybernetické bezpečnosti.

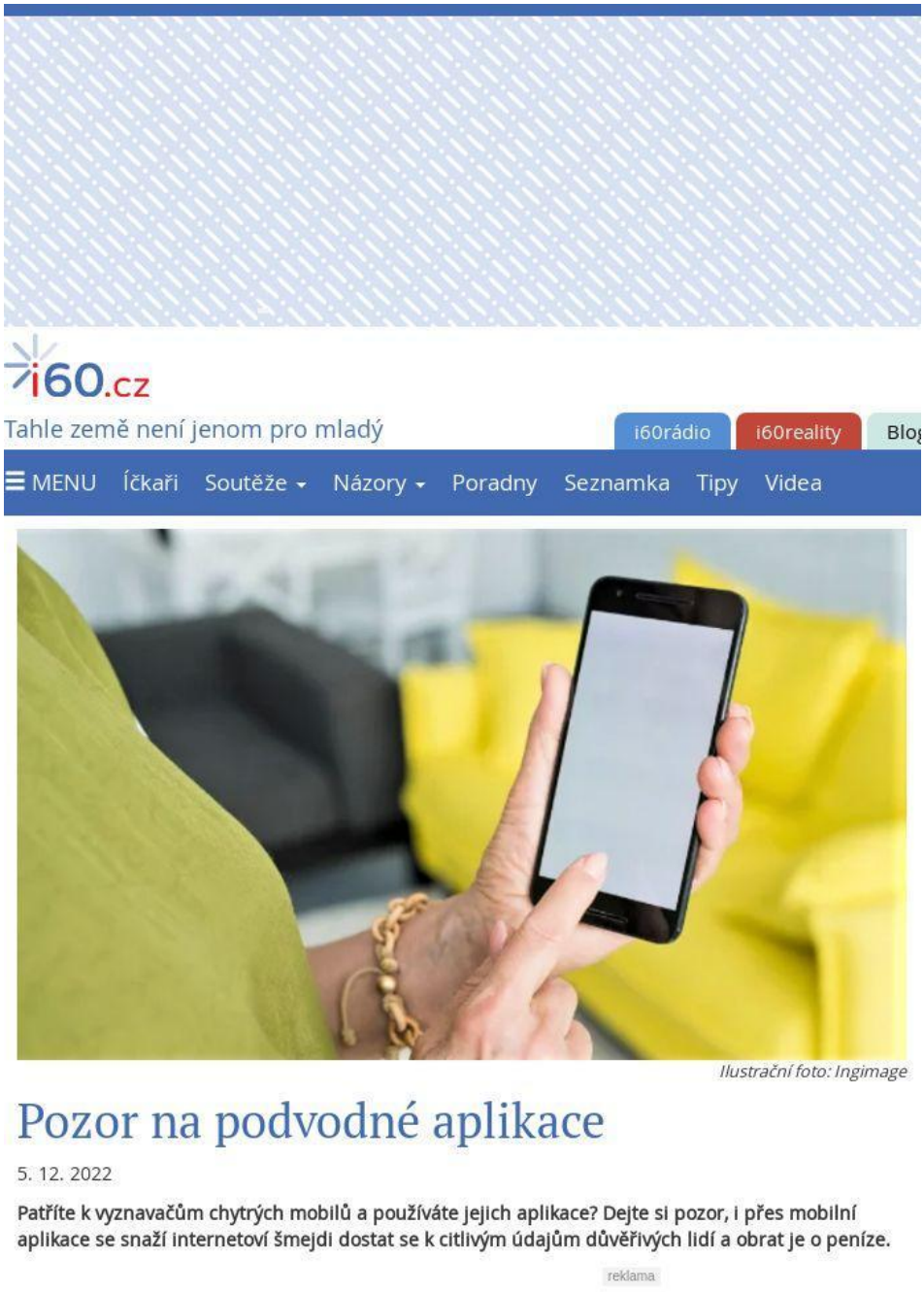
141. Pozor na podvodné aplikace

Online ● i60.cz (Jiné) ● 5. 12. 2022, 10:25

Vydavatel: **i60 Publishers, s.r.o. (cz-24214868)**

Dosah: 16 724 ● GRP: 0.19 ● OTS: 0.00 ● AVE: 18532.40 Kč

Odkaz: https://www.i60.cz/clanek/detail/31531/pozor-na-podvodne-aplikace



Jedním z velmi aktuálních triků útočníků jsou i malwarem infikované mobilní aplikace či jejich aktualizace, které si nejčastěji stáhnete z neoficiálních obchodů s aplikacemi a webových stránek. Výjimkou ale nejsou ani podvodné aplikace nainstalované přímo z oficiálního obchodu.

Pokud v telefonu nemáte nainstalovaný bezpečnostní software, který by vás varoval, a při instalaci aplikaci udělíte vysoká oprávnění – například aplikaci pro nahrávání hovorů i přístup k fotoaparátu či SMS – dokáže aplikace odcizit vaše přihlašovací údaje do bankovnictví, obejít dvoufázové ověření či získat potvrzovací SMS.

Na podvodné aplikace upozornila nedávno například bezpečnostní firma Avast. Podle ní bylo v internetových obchodech ke stažení více než 150 podvodných aplikací, které z uživatelů lákaly peníze prostřednictvím prémiových SMS. Aplikace měly více než deset milionů stažení a mimo jiné se vydávaly za přizpůsobené klávesnice, skenery QR kódů, editory videí a fotografií, blokátory nevyžádaných hovorů, filtry fotoaparátu a hry. Češi si je stáhli 1600 krát a Slováci méně než 500 krát. Škody jdou do stovek milionů...

„Jedná se o aplikace, které po stažení například kontrolují polohu zařízení uživatele, telefonní číslo a tak dále, aby zjistily, v jakém jazyce půjde podvod uskutečnit. Po otevření aplikace je uživatel požádán o zadání telefonního čísla, případně e-mailové adresy a dalších citlivých údajů. Základním pravidlem ovšem je, že do internetového bankovnictví se člověk přihlašuje jen proklikem ze skutečné domovské stránky banky, ne přes odkaz v mailu nebo sms. Skutečná banka, energetika nebo e-shopy po klientech nikdy nechtějí žádné přístupy do bankovnictví, jeho zákaznických účtů nebo jiné citlivé údaje, které se podvodníci snaží od klientů dostat„“ přiblížil pro Deník Martin Schreier, mluvčí společnosti ČEZ, která má, podobně jako banky, s podvodným jednáním šmejdů také zkušenosti. Firma proto loni spustila provoz vlastního bezpečnostního dohledového centra. Systém zachytil asi dvacet tisíc útoků.

Jak podvodné aplikace poznat a jak se jim bránit?

1. Stahujte aplikace jen z důvěryhodných zdrojů – nejlépe Google Play či App Store.
2. Před stažením věnujte pozornost recenzím a hodnocení aplikace a tomu, zda nejste mezi prvními, kdo aplikaci stahuje.
3. Ověřte si i jméno vývojáře a to, zda vyvinul více aplikací. Podívejte se i na ostatní aplikace, na jejich recenze a počet stažení.
4. Při udělování oprávnění aplikacím se řiďte heslem, že méně je někdy více. Dobře si rozmyslete, zda stahovaná aplikace opravdu potřebuje přístup k vašim fotkám, kontaktům, úložišti, poloze apod.

Kybernetičtí zločinci se při pokusech vás okrást neustále zdokonalují. K vašim penězům se již dávno nesnaží dostat jen s pomocí e-mailů slibujících snové dědictví či falešných stránek. Jaké jsou nejčastější typy internetových obchodů? Podívejte se na Kybertest, edukativní projekt České bankovní asociace.

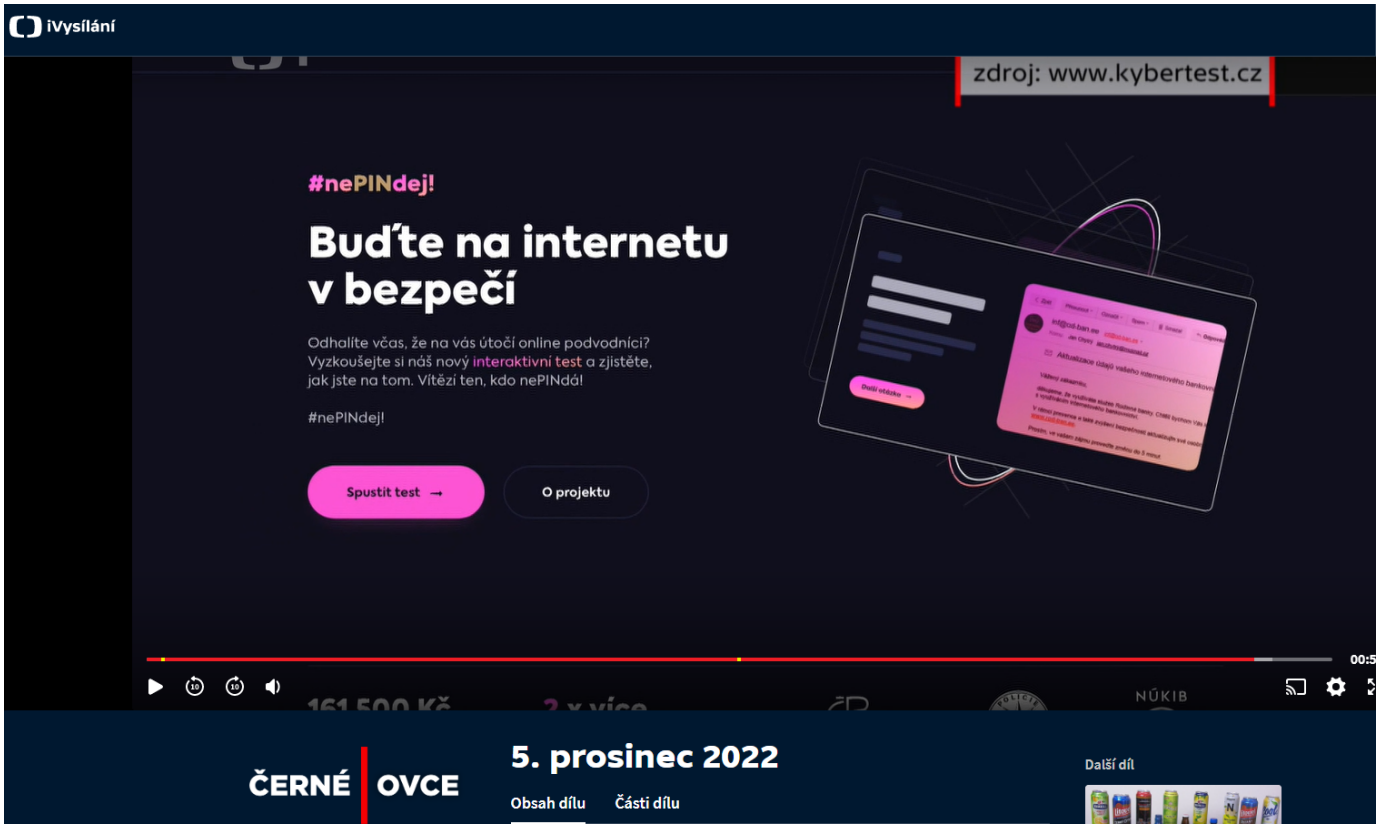
142. Černé ovce: 5. prosinec

Televize ● Černé ovce (ČT1) ● 5. 12. 2022, 17:40

Vydavatel: **ČESKÁ TELEVIZE (cz-00027383)**

Dosah: 335 065 ● GRP: 3.72 ● OTS: 0.04 ● AVE: 5360202.34 Kč

Odkaz: https://www.ceskatelevize.cz/porady/1097429889-cerne-ovce/222452801081205/



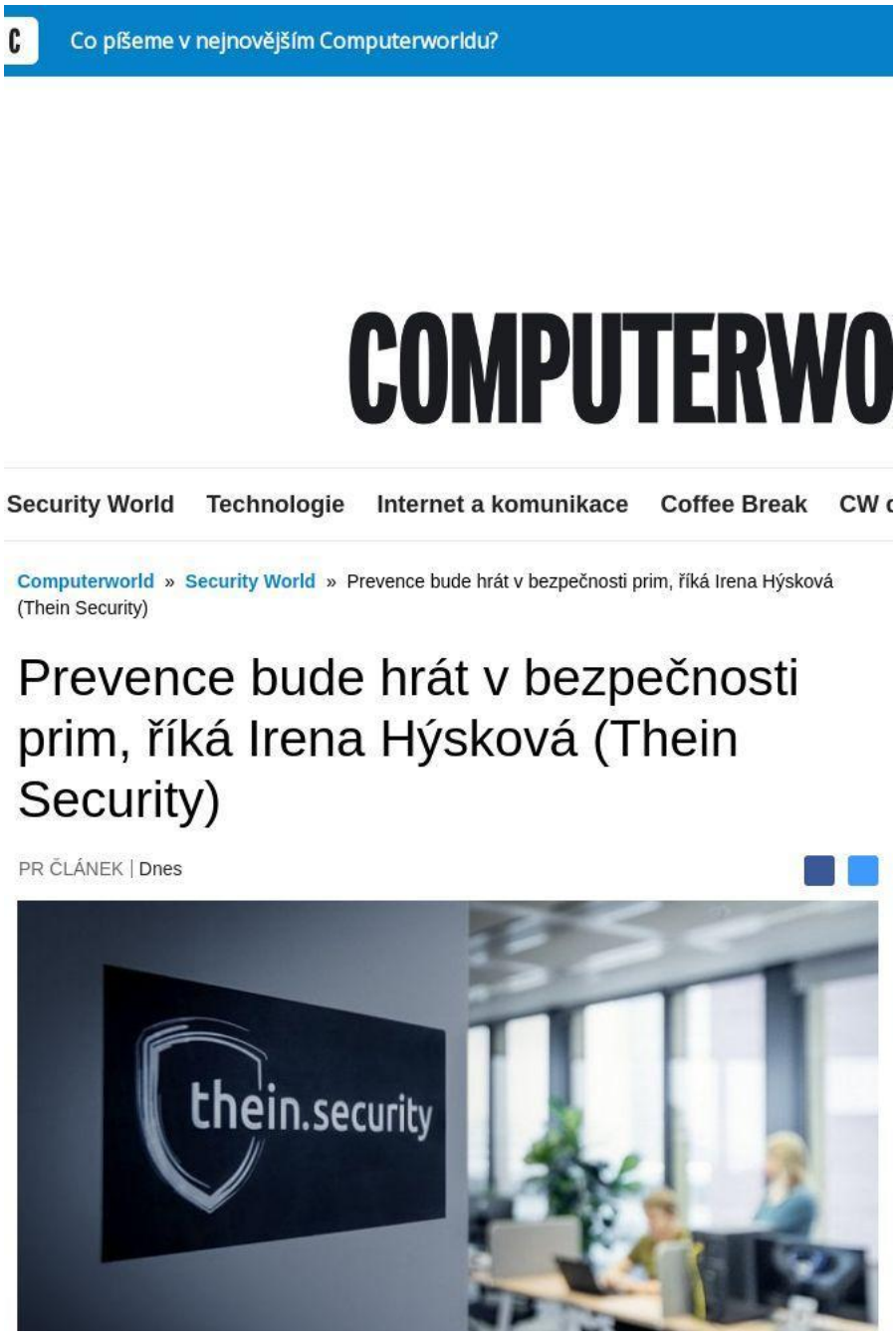
143.Prevence bude hrát v bezpečnosti prim, říká Irena Hýsková (Thein Security)

Online ● computerworld.cz (IT / Technologie) ● 8. 12. 2022, 0:00

Vydavatel: **Internet Info DG, a.s. (cz-00565211)**

Dosah: 610 ● GRP: 0.01 ● OTS: 0.00 ● AVE: 5674.48 Kč

Odkaz: https://www.computerworld.cz/clanky/prevence-bude-hrat-v-bezpecnosti-prim-rika-irena-hyskova-thein-security/



Jaké jsou současné výzvy v oblasti kybernetické bezpečnosti, vysvětluje Irena Hýsková, výkonná ředitelka společnosti Thein Security, společně se svými kolegy Ondřejem Remešem, cyber security managerem, a Oldřichem Gosmanem, manažerem pro SOC.

V poslední době se stále častěji mluví o nové evropské bezpečnostní směrnici NIS2. Co mohou firmy od ní očekávat?

Irena Hýsková (IH): NIS2 navazuje na předchozí evropskou normu NIS z roku 2016. Cílem je zvýšit kybernetickou odolnost firem kritické infrastruktury a také dalších významných podniků, a to zejména v oblasti prevence. Lze čekat, že se dotkne přibližně šesti tisíc soukromých i státních subjektů.

Mezi možná preventivní opatření patří např. kontinuální školení zaměstnanců, kvalitní firewally, zabezpečení koncových zařízení, vícefaktorové ověřování nebo produkty antiDDoS. Řešení existuje celá řada, a naše firma má tým, který je dokáže aplikovat.

NIS2 také představuje vyšší odpovědnost statutárních orgánů jednotlivých společností a na rozdíl od NIS se zaměřuje právě na zmíněnou prevenci. Doporučuji každému zodpovědnému manažerovi sledovat stránky úřadu NÚKIB pro nejaktuálnější vývoj.

Hrozí v rámci NIS2 firmám nějaké sankce?

IH: Určitě ano, směrnice navíc stanovuje maximální hranice pokut poměrně vysoko (v max. výši deset milionů eur nebo dvě procenta ze světového obratu). NÚKIB na svých stránkách také uvádí, že lze očekávat proporcionální pokuty zohledňující povahu porušení, hrozící škody apod. Firmy by se tedy měly zamyslet nad tím, co jim může nesplnění požadavků NIS2 přinést. Nejde jen o finanční sankce, ale především o dopad případného kybernetického útoku na samotnou organizaci (ztráta firemní reputace, dat, výpadek provozu výrobních kapacit aj.)

Jsou firmy podle vás schopné požadavkům NIS2 vyhovět svépomocí?

IH: K NIS2 budou určitě vydané metodické pokyny k jejímu naplňování. Jde však stejně jako u účetnictví o složitou problematiku. Firmy mají zákonnou povinnost účetní agendu vést a zároveň ji potřebují ke svému podnikání. A podle složitosti účetní agendy volí, jestli se jí budou zabývat samy, zaměstnají interního specialistu nebo najmou externí, specializovaný subjekt.

Ne každá společnost si ale může dovolit vlastní tým odborníků na kybernetickou bezpečnost, tak aby si mohly všechny oblasti tohoto oboru pokrýt vlastními silami. V každém případě tedy doporučuji kontaktovat specializované firmy, které se kybernetickou bezpečností zabývají, a přinejmenším s nimi zkonzultovat vlastní plány na implementaci NIS2.

Existují nástroje, které by firmám pomohly splnit zvýšené požadavky na ochranu dat, aniž by musely zaměstnávat množství bezpečnostních expertů?

IH: Je zjevné, že na trhu práce právě tato specializace dlouhodobě chybí. Automatizace v oblasti detekce a reakce na bezpečnostní události – systémy SOAR – je dnes jedna z mála šancí, jak potřebu na velké množství lidí v oblasti kybernetické bezpečnosti nějak snížit.

Naštěstí existují firmy, mezi něž patří i ta naše, které nedostatek expertů dokážou vhodně doplnit nástroji renomovaných společností.

Thein Security spolupracuje například s Palo Alto Networks, u níž je držitelem nejvyšší dodavatelské certifikace Diamond Innovator a je jediným autorizovaným servisním centrem pro ČR/SR, dále s firmami Netscout, Microsoft a dalšími. A od společnosti PANW máme v portfoliu například Cortex XDR, což je produkt, který detekuje i vyšetřujte případné hrozby a nežádoucí aktivitu dokáže zastavit v reálném čase.

Dalším vhodným řešením je NGFW, proaktivní nástroj umožňující hloubkovou kontrolu provozu včetně šifrované komunikace na úrovni síťového provozu, aplikací, uživatelů a obsahu přenášených dat. Umožňuje tak předcházet známým i neznámým hrozbám. A od společnosti Netscout pak nabízíme řešení antiDDoS Arbor, které se globálně používá v malých i velkých firmách.

Organizační bezpečnost ale může mít na celkové zabezpečení firem větší vliv než použité technologie, je to tak?

Ondřej Remeš (OR): To je pravda, ale systémy řízení informační bezpečnosti – ISMS – jsou výsadou převážně velkých firem, případně organizací, které potřebují prokázat soulad se standardy ISO 27000 nebo se zákonem o kybernetické bezpečnosti (ZoKB). V menších firmách je bohužel zatím dobrovolná adopce těchto standardů spíše výjimkou. Často je to také doprovázeno nedostatkem bezpečnostního personálu. Zároveň však vnímáme trend stále častějšího vzdělávání zaměstnanců a následného ověřování znalostí pomocí simulovaných phishingových kampaní. I to je aktivita, kterou se snažíme u našich zákazníků adresovat a pomoci vyřešit.

Osvěta je určitě klíčem k lepší bezpečnosti – co ale kromě školení může zlepšit obecné povědomí o kybernetické ochraně?

OR: Podle naší zkušenosti má smysl jen průběžné školení zaměstnanců, které posouvá jejich znalosti, ale zároveň nevyžaduje hodiny před monitorem. Důležitá je i zpětná vazba formou testů, kvízů nebo simulovaných phishingových kampaní, které prokážou aktuální úroveň znalostí a mohou ovlivnit strukturu a cílení školicího plánu. Stěžejní je také komunikace v organizaci. Motivace pro jednotlivce je různá a je důležité pochopit, že znalosti jsou k užitku také v soukromí. Pro širokou veřejnost pak existují formy testů nebo školení pořádané neziskovými nebo profesními organizacemi. Příkladem může být Kybertest.cz organizovaný Českou bankovní asociací, který za přispění Thein Security cílí na bezpečné používání elektronického bankovnictví.

Proč ale i vyškolení lidé útokům kyberzločinců dokážou podlehnout?

OR: I když člověk prochází takovým školením – a jak jsem zmínil, to je kontinuální proces – tak se může stát, že nerozpozná pokus o hackerský útok. Nicméně toto riziko se s pravidelnou edukací výrazně redukuje.
V kyberbezpečnosti bohužel žádné opatření nedává jistotu, že k úspěšnému útoku nedojde. Právě dobře nastavené firemní procesy, existující bezpečnostní monitoring v rámci střediska bezpečnostních operací (SOC) a kontinuální vzdělávání s velkou pravděpodobností zaručí, že útok bude buď neúspěšný, nebo se včas a rychle objeví i vyřeší.

Právě phishing a sociální inženýrství představují hrozbu, proti kterým se špatně brání. Jaké by měly být zásady, jak jí čelit?

Oldřich Gosman (OG): Na phishingovou kampaň nepotřebujete žádné sofistikované nástroje, zjednodušeně řečeno vám stačí jen e-mail. Je mnohem snazší a levnější při útocích překonávat „běžný“ lidský faktor a namísto prolamování bezpečnostních technologií si o citlivé informace jednoduše říct. Phishing se ale v dnešní době už netýká jen e-mailu, stejné riziko číhá i v případě tzv. instant messagingu, např. skrze Facebook Messenger, WhatsApp apod. Přes tyto platformy se šíří podvodné zprávy – i zdánlivě od přátel – vyzývající třeba k přeposlání citlivých informací, kliknutí na falešný odkaz či přílohu.

Phishing využívá známé životní situace, kdy útočník chce od uživatele získat cenné informace. A ty zásady? **Vzdělávejte se –** naučíte se, jak chránit sebe a svoji firmu. **Sdílejte na internetu co nejméně informací.** Dnešní útoky jsou vizuálně bezchybné, gramaticky správné a mají cílený, přesvědčivý obsah jak z hlediska technického, tak i psychologického. Chraňte své účty a zařízení silnými hesly – **používejte MFA**,tedydvoufázová ověření pomocí kódu v SMS nebo otisku prstu.

Firmám, které mají problémy s vlastním zajištěním bezpečnosti, mohou

pomoci SOC – střediska bezpečnostnich operaci. Co všechno může SOC zajistit a jak je to finančně náročné?

OG: SOC zájemcům doručí komplexní dodávku školených odborníků – SOC analytiků, technologií – dohledové nástroje typu XDR, EDR, SIEM, XSOAR a procesů. Také definují spolupráci a formalizují postupy v případě nálezů, incidentů a detekcí. Je to vlastně takový mix organizačních a technických opatření s cílem snížit útočnou plochu a detekovat anomálie. Finanční náročnost je pak závislá na požadavcích – některé firmě stačí dohled v pracovní dobu v režimu 5 × 8, jiná zase požaduje plný dohled 24 × 7 × 365, a to je cenově jiná služba.

Není pro firmu složité využít služby SOC?

OG: Složité to není, ale nejde o prostou „instalaci" technologií. Je to proces, který se vyvíjí s měnícími se potřebami zákazníka a bezpečnostní situací. Podle mne je klíčové prvotní rozhodnutí. V ideálním případě je k dispozici technická role, např. jde o architekta bezpečnosti a bezpečnostního ředitele, někoho s rozhodovací kompetencí.

V rámci našeho standardního postupu je klíčový tzv. onboarding, kdy se udělá vstupní analýza, definuje výchozí stav a zmapují aktiva firmy. Na to navazuje pilotní provoz SOC, definují se bezpečnostní alerty a jejich řešení. Tato fáze je na součinnost obou stran nejnáročnější. Ve všech těchto činnostech jsme v rámci best practice schopní firmám pomoci, ale finální rozhodnutí bude vždy na vlastníkovi. Výsledná opatření musejí podporovat procesy firmy a zároveň respektovat bezpečnostní požadavky – ani jeden ze zmíněných pohledů by neměl převažovat.

O Thein Security

Thein Security, součást skupiny Thein, nabízí komplexní služby spojené s ochranou firem v kyberprostoru včetně prevence úniku citlivých dat, obrany proti sofistikovaným útokům, detekce neznámého malwaru nebo aktivní ochrany proti DDoS útokům. Firma má vlastní bezpečnostní středisko SOC pro zákazníky, kteří se chtějí soustředit na své podnikání, ale současně vyžadují prvotřídní dohled nad ochranou svých dat v kyberprostoru.

144. Co dokážou podvodné wifi? Stačilo projít kolem a data byla pryč

Online ● seznamzpravy.cz (Zprávy / Politika) ● 11. 12. 2022, 20:21

Vydavatel: **Seznam.cz, a.s. (cz-26168685)** ● Autor: **Karolína Štuková**

Dosah: 1 702 492 ● GRP: 18.92 ● OTS: 0.19 ● AVE: 79177.75 Kč ● Interakcí: 71

Odkaz: https://www.seznamzpravy.cz/clanek/tech-technologie-co-dokazou-podvodne-wifi-stacilo-projit-kolem-a-data-byla-pryc-220997

Seznam Zprávy

ZPRÁVY BYZNYS TECH P

TECH TECHNOLOGIE VĚDA INTERNET NÁVODY

Krize a inflace? Lidé vzali obchody útokem, za dárky utrácejí více než loni

Unikátní model. Kdo vyhraje sněmovní volby

Nejvíc se bojím, že skončí svět, říká mladá Francouzka

Češi vybírají peníze na Viktory. Pomůžou Ukrajincům „zavřít nebe“

Zprávy » Tech » Technologie » Co dokážou podvodné wifi. Stačilo projít kolem a data byla pryč

Co dokážou podvodné wifi. Stačilo projít kolem a data byla pryč

20:21

Letiště, obchodní centrum nebo hotel. Tam všude je uživatelům k dispozici veřejná wifi. Pokud ale není dostatečně zabezpečena, může se velmi snadno stát cílem podvodníků. Spolu s ní jsou v ohrožení také připojená zařízení.

Mobilní zařízení už dnes nejsou schránkou pouze pro ukládání telefonních čísel, naopak v sobě uchovávají mnoho citlivých údajů. Od fotografií přes kontaktní údaje, hesla až po přístupy do on-line bankovnictví.

To všechno jsou přesně informace, které internetové podvodníky zajímají. Za účelem jejich získání mohou využít mimo jiné i veřejnou wifi síť.

„Obecně jde o fakt, že nikdy nevíte, kdo veřejnou wifi síť skutečně provozuje a jaké má úmysly. U přistupování na webové stránky, které nepoužívají šifrování, může dojít velmi snadno k odchycení celé komunikace – tedy všeho, co si na dané webové stránce uživatel prohlíží, odesílá, nebo třeba jaké vyplňuje osobní údaje,“ vysvětluje Jan Pinta, expert na kybernetickou bezpečnost v Thein Security.

Jak poznat podvodnou aplikaci na mobilu

5. 12. 16:59

Může také podle jeho slov docházet k odposlechu komunikace či doručení škodlivých souborů prostřednictvím takzvaných „Man in the Middle“ útoků, tedy takových, kdy se někdo další, bez vědomí uživatele, dostane mezi jeho počítač a internet.

„Veřejné sítě se mohou také často vydávat za na první pohled známé sítě, například některého jídelního či kavárenského řetězce, přičemž jde pouze o další podvod a nalákání oběti. Na veřejných sítích se také často objevuje snaha o vylákání údajů k platební kartě nebo k instalaci softwaru, který následně komunikaci odposlouchává,“ doplňuje Pinta.

Kampaň #nePINdej!

- Patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti u nás. Zapojily se jak orgány státní správy, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají.
- Kromě ČBA a Policie České republiky i Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), itego, a. s., Cisco, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy.
- Mediálními partnery jsou Česká televize (hlavní mediální partner), Seznam Zprávy, Deník a CineStar.

A cílovou skupinou je podle odborníků prakticky každý uživatel mobilního zařízení.

„Ta se k takové zákeřné wifi dokážou připojit i sama, aniž by to jejich uživatel věděl, nebo chtěl. Stačilo mít třeba telefon v kapse, projít kolem konferenční místnosti, kde jsem zrovna dělal ukázku takového nechtěného připojení, telefon se sám připojil, zjistil, že má připojení k internetu, a stáhl si e-maily, a pokud to bylo po nezabezpečeném spojení, mohl jsem

zachytit i heslo k poštovní schránce," popisuje z vlastní zkušenosti Michal Špaček, bezpečnostní expert.

Jistou mírou ochrany může být pro internetové uživatele podle Jana Pinty, experta na kybernetickou bezpečnost v Thein Security, určitá forma technického zabezpečení.

U domácího zařízení to bude nejčastěji antivirové řešení, u pracovního pak stanice EDR nebo XDR, které slouží k ochraně koncových stanic před škodlivým kódem a průnikem útočníka.

„Ovšem žádná technologie nás nemůže ochránit na sto procent. Důležitý je především zdravý rozum, alespoň základní povědomí o nástrahách a kybernetických útocích, které na nás mohou číhat, a také rozumět praktikám sociálního inženýrství," dodává Pinta.

Jak podvodné wifi sítě poznat a jak se jim bránit?

1. Věnujte pozornost názvu nabízené veřejné wifi sítě. Pokud se jmenuje „Public Plzeň", ale vy v Plzni nejste, je to podezřelé.
2. Jakmile je u veřejné wifi znak otevřeného zámečku, mějte na paměti, že vaši komunikaci může kdokoli „odposlouchávat".
3. Nepovolujte automatické připojování k neznámým wifi sitím.
4. Pro zvýšení své bezpečnosti používejte VPN – virtuální privátní síť.
5. Pokud si nejste jisti zabezpečením používané wifi sítě, nezadávejte nikam své citlivé údaje.
6. Za připojení k veřejné wifi síti nikdy nic neplaťte ani nesdělujte své platební údaje nebo jiné osobní údaje, například rodné číslo nebo číslo občanského průkazu.

Zdroj: Kybertest

Pozitivní zprávou však je, že počet útoků na veřejné wifi v posledních letech neroste, spíše naopak.

„Počet podvodů za posledních asi 10 let rapidně klesl až k nule, a to díky masivnímu rozmachu šifrování nejen webových stránek, ale i dalších používaných aplikací, jako je například e-mail," informoval bezpečnostní expert Michal Špaček.

Například v prohlížeči Chrome má aktuálně už přes devadesát procent načítaných stránek šifrované a zabezpečené spojení. Ještě v roce 2015 to byla zhruba třetina.

Také výhled vypadá podle Špačka pozitivně. „Podobných útoků již nebude přibývat, v blízké budoucnosti ten počet klesne na nulu," uvedl.

Seznam Zprávy jsou mediálním partnerem **kampaně #nePINdej.**

145. Policie ČR spolu s bankami přicházejí se vzdělávací kampaní upozorňující na kyber podvody

Online ● regionblanensko.cz (Regionální zprávy) ● 14. 12. 2022, 4:15

Vydavatel: **BitWave Consulting s.r.o. (cz-24159531)**

Dosah: 106 ● GRP: 0.00 ● OTS: 0.00 ● AVE: 1453.25 Kč

Odkaz: https://www.regionblanensko.cz/zpravy/aktualne/21685--Policie-CR-spolu-s-bankami-prichazeji-se-vzdelavaci-kampani-upozornujici-na-kyber-podvody.html

Regionální zpravodajství

Policie ČR spolu s bankami přicházejí se vzdělávací kampaní upozorňující na kyber podvody

Policie ČR
dnes 14.12.2022

Ilustrační foto
Autor: kybertest.cz

Policisté varují před podvodníky, kteří cílí na klienty bank. Počet takových útoků se za poslední dva roky zvýšil čtyřnásobně. **Škody jdou do stovek milionů.** Police České republiky se připojila k rozsáhlé vzdělávací kampani **#nePINdej!** České bankovní asociace a dalších partnerů, která upozorňuje na sílící nebezpečí podvodů na internetu.

Obětí podvodníka se nedávno stal například šestačtyřicetiletý muž z Blanenska. Vše se odehrálo podle osvědčeného scénáře. **Na začátku byl telefonát a oznámení, že při obchodování s**

kryptoměnou získal skoro čtyři tisíce dolarů, tedy skoro sto tisíc korun.

„Benefit bylo nutné převést na jeho účet. Muž tedy ochotně vyplnil emailem zaslaný podvodný formulář a poskytl potřebné údaje. Tím umožnil podvodníkovi především neomezený přístup k bankovnímu kontu. Z něj zmizelo více než sto tisíc korun. Navíc podvodník sjednal půlmiliónovou půjčku. Z možného zisku se tak vygenerovala velká ztráta," popsal případ policejní mluvčí Bohumil Malášek.

Podobně skončilo obchodování s kryptoměnou pro šestašedesátiletou ženu.

I ona poskytla potřebné údaje.

Dále zaplatila vstupní poplatek a nechala si nainstalovat program na vzdálenou správu počítače. „Pak už jen s odborníkem na kryptoměny sledovala, jak tento obchoduje.

Výsledkem čtyřdenní činnosti byla ztráta více než třiceti tisíc korun. Potom podvodník komunikaci ukončil a žena pochopila, že se stala jeho obětí," doplnil policejní mluvčí.

Z dat České bankovní asociace vyplývá, že na jednoho poškozeného klienta připadá průměrná škoda ve výši 161 500 korun. U vishingu, neboli případů podvodného navolávání, jsou částky až čtvrtmilionové.

Klíčovým prvkem kampaně s názvem #nePINdej! (kreativní tvorba ze slov PIN nedej) je **interaktivní vzdělávací www.kybertest.cz, který zábavnou formou seznámí veřejnost s nejčastějšími kybernetickými podvody a naučí ji, jak je rozpoznat a jak jim předcházet.**

„**Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin**. Kybernetická kriminalita již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Kampaň proto cílí na širokou veřejnost počínaje dětmi a mladistvými přes dospělé až po seniory.

Otázky v testu jsou tedy generovány dle věku uživatele," upřesnila policejní komisařka Lenka Koryťáková.

V kybertestu jsou simulovány podvodné SMS, zobrazovací okna k připojení k WIFI sítím, phishingové emaily, zvukové nahrávky podvodných telefonů a mnohé další, tak, aby si je každý uživatel moderních technologií mohl bezpečně vyzkoušet.

Testové otázky byly připravovány odborníky na základě reálných případů, jimiž se podvodníci snaží své oběti nachytat.

Pachatelé se při těchto útocích snaží překonávat zejména lidský faktor a pod

nejrůznějšími legendami využívají nátlaku, strachu a časové tísně pro záchranu peněz nebo pro realizaci finanční transakce.

Mezi nejčastější podvodné legendy patří:

1) Podvodné navolávání: Pachatelé se vydávají například za bankéře, policisty, pracovníky technické podpory a snaží se z lidí pod vlivem strachu vylákat peníze, nebo vzdálený přístup do zařízení oběti, který následně zneužije.

2) Nabídka výhodných investic: Přesvědčivá lákavá reklama a manipulativní jednání.

Cílem pachatele je vylákat z oběti co možná nejvíce finančních prostředků a využívá k tomu přirozenou ziskuchtivost každého z nás.

3) Reverzní inzertní podvody: Pachatel zareaguje na váš inzerát. Podstrčí vám fiktivní platební bránu, kde vyplníte citlivé bankovní údaje a místo peněz za inzerované zboží přicházíte o všechny úspory.

4) Podvody typu Nigerijské dopisy: Princip, který funguje už více jak 100 let. Pachatelé sázejí na kvantitu. Vždy se najde někdo, kdo se nechá nachytat na slibovanou cennou zásilku nebo domnělou pomoc. Často zde hraje velkou roli láska.

5) Klasické podvody typu phishing a smishing: Stále dokonalejší a složitě rozpoznatelné podvodné emaily a SMS nabídky. Na první pohled již nenajdeme podezřelé znaky.

„**Stále častější praktikou jsou v současné době tzv. reverzní inzertní podvody.** Terčem útočníků jsou v takovém případě především prodávající, kteří si zvolí jako platební metodu ‚bezpečnou platbu', tedy zaslání peněz z karty na kartu, prostřednictvím peněženky zvoleného bazaru. Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k účtům a do jejich internetového bankovnictví.

Mají zájem zboží prodat, a aby toho co nejdříve docílili, slepě spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně, a s vírou, že získají peníze za prodávané zboží. Opak je bohužel pravdou, o všechno přijdou," upozornila Koryťáková.

Základní rady, jak nenaletět

Poznej svého nepřítele. Seznamuj se s aktuálními hrozbami a trendy v online podvodech.

Nikdy se nenech od pachatele do ničeho tlačit a vše si pečlivě promysli

Jakmile je zpráva, e-mail, SMSka, nebo telefonát neočekávaný, tak je podezřelý.

Vždy se zamysli nad tím, kam vypisuješ citlivé údaje, nebo přeposíláš peníze.

Když si nejsi absolutně jistý, tak vždy raději vše ověř jinou cestou.

Pamatuj si, že pachatel dokáže napodobit jakékoliv tel. číslo, či e-mailovou adresu.

Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, komu zcela nedůvěřuješ.

Kupující na inzertních portálech nikdy nepotřebuje citlivé údaje z tvé platební karty.

Vyzkoušej si www.kybertest.cz a zjisti, kde máš mezery.

Článek byl převzat se souhlasem vydavatele Zpravodaje města Blanska. Titulek je redakční.

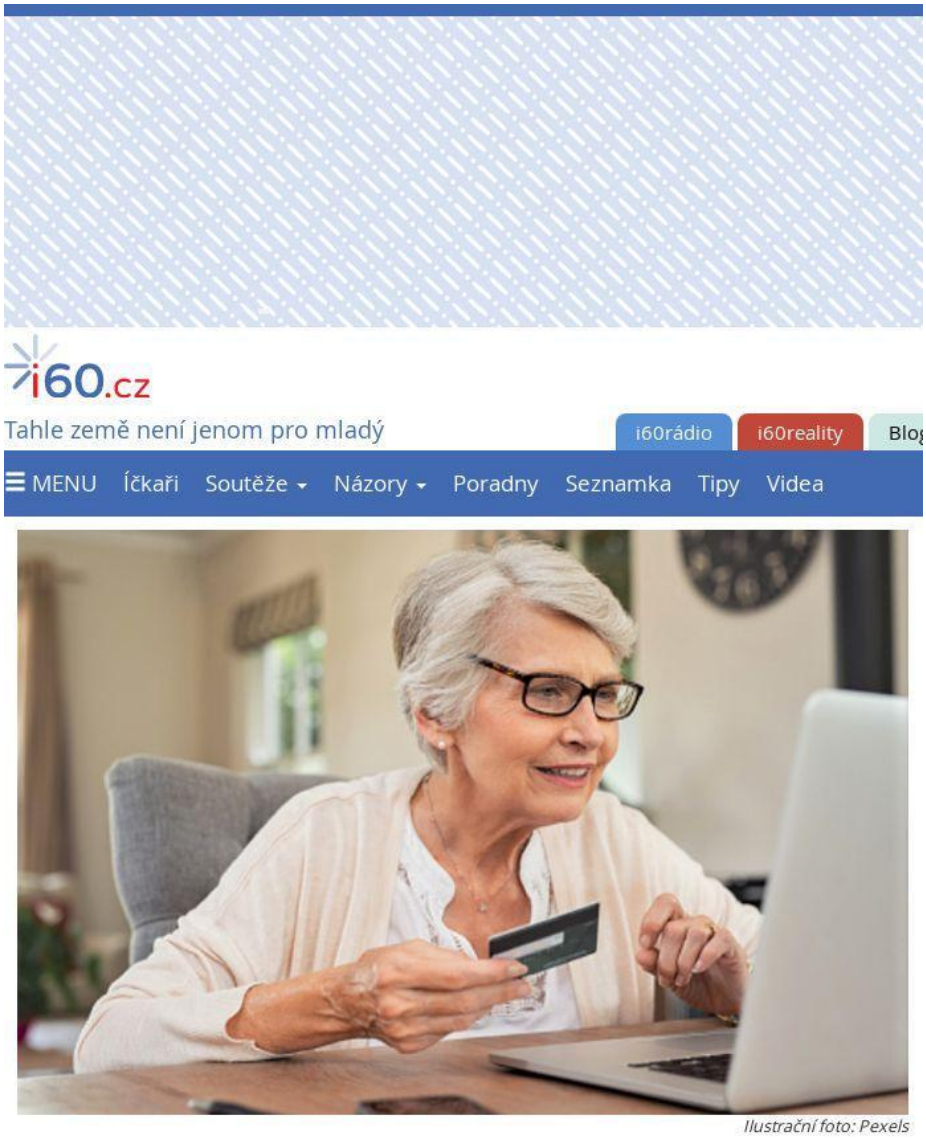
146. Šmejdi lákají peníze přes podvodné platební brány

Online ● i60.cz (Jiné) ● 14. 12. 2022, 5:50

Vydavatel: **i60 Publishers, s.r.o. (cz-24214868)**

Dosah: 16 724 ● GRP: 0.19 ● OTS: 0.00 ● AVE: 18532.40 Kč

Odkaz: https://www.i60.cz/clanek/detail/31533/smejdi-lakaji-penize-pres-podvodne-platebni-brany



Ilustrační foto: Pexels

Šmejdi lákají peníze přes podvodné platební brány

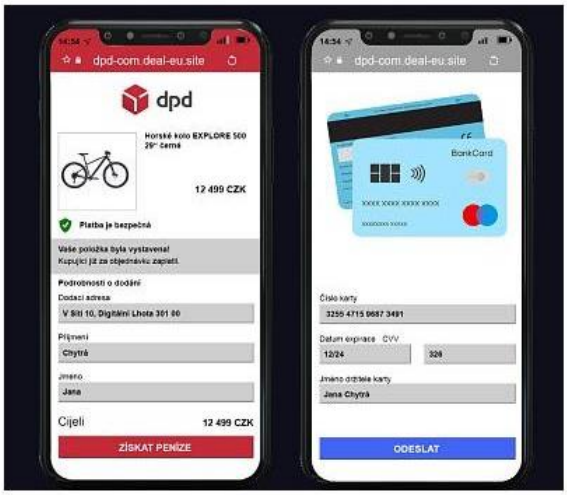
14. 12. 2022

Prodávali jste někdy něco na inzertních serverech? Potom si mohli podvodníci vyhlédnout i vás a vylákat z vás podvodem peníze. Přesto, že se jedná o celkem nový druh podvodu, setkáváme se s

Podvodníci získají z inzerátu vaši e-mailovou adresu nebo telefonní číslo a kontaktují vás prostřednictvím aplikací WhatsApp nebo Messenger s předstíraným zájmem o koupi inzerovaného zboží. Během konverzace vás navádějí k tomu, abyste uhradili poplatek za přepravu zboží, kterou kupující (tedy podvodník) zajistí, a to přes platební bránu jimi domluveného dopravce. V odkazu na falešnou platební bránu, který vám ve zprávě zašlou, po vás chtějí vyplnit citlivé údaje o platební kartě včetně PIN, případně přístupové údaje do online bankovnictví včetně hesla a bezpečnostního kódu z autorizační SMS. A neštěstí je hotovo!

Díky získaným údajům se podvodník dostane do vašeho online bankovnictví, kde provede převod finančních prostředků na svůj bankovní účet, nebo na základě zjištěných údajů z platební karty provede její tokenizaci a následně v bezkontaktním bankomatu vybere z vašeho účtu peníze.

Ukázka podvodné platební brány:



Podle Michala Čarného, generálního ředitele společnosti Mastercard pro Česko a Slovensko s rostoucím objemem online transakcí, který ještě zesílil během pandemie covidu, úměrně roste i počet pokusů o podvody. „Pro většinu útoků platí, že jsou vedeny v co největším rozsahu a bývají obvykle automatizované," uvádí Čarný. „Objevují se ale i sofistikované útoky, kdy se útočníci snaží co nejvíce napodobit obvyklé lidské chování nebo se pokouší nakupujícího zmanipulovat či uvést v omyl," uvedl Michal Čarný pro Seznam Zprávy. Obecně ale podle šéfa Mastercard platí, že platby kartou jsou v současnosti historicky vůbec nejbezpečnější. Je to proto, že dnes funguje celá řada nástrojů založených na datech a umělé inteligenci, které jsou schopny identifikovat a předejít zneužití karet kdekoliv na světě.

Jak podvodné platební brány poznat a jak se jim bránit?

1. Pokud na inzerát reaguje cizinec, zbystřete.
2. Buďte na pozoru, když kupující požaduje nestandardní způsob dopravy nebo způsob platby. Příkladem je zajištění jeho platby „přepravní společností", která peníze uvolní, až bude zboží na cestě, nebo platební brána, která vyžaduje údaje z platební karty prodávajícího.
3. Nereagujte na požadavky kupujícího, že zaplatí přes neznámé služby různých nebankovních platebních společností nebo v kryptoměně.
4. Nepřistupujte na platbu nedoplatků, přeplatků či kaucí a nikam nezadávejte své platební údaje, například číslo karty. Kupující má platit vám, ne vy jemu.

Zdroj: Česká bankovní asociace a Seznam Zprávy

Jako užitečný návod, jak rozpoznat podvodné útoky, může posloužit Kybertest, který připravila Česká bankovní asociace. V něm si každý může vyzkoušet svou zdatnost v kybernetické bezpečnosti.

147. Množí se lákavé inzeráty. Bez vašeho vědomí z vás udělají podvodníka

Online ● seznamzpravy.cz (Zprávy / Politika) ● 15. 12. 2022, 8:28

Vydavatel: **Seznam.cz, a.s. (cz-26168685)** ● Autor: **Karolína Štuková**

Dosah: 1 702 492 ● GRP: 18.92 ● OTS: 0.19 ● AVE: 79177.75 Kč ● Interakcí: 129

Odkaz: https://www.seznamzpravy.cz/clanek/tech-technologie-mnozi-se-lakave-inzeraty-bez-vaseho-vedomi-z-vas-udelaji-podvodnika-221300

Ilustrační foto.

8:28

Jak se z oběti internetového podvodu může stát podvodník? Trik je jednoduchý a oběť o tom, že páchá trestnou činnost, ani neví. Počet takových podvodníků navíc dlouhodobě roste.

Článek si také můžete poslechnout v audioverzi.

Nejen, že v důsledku počítačové kriminality oběti podvodů mohou přijít o své úspory, v některých případech se mohou stát i její součástí, podílet se na ní, a tedy být za ni i trestně zodpovědní.

Jedním ze způsobů, jak se podvodníci snaží uživatele k nelegální činnosti přemluvit, jsou podezřele výhodné nabídky práce, které slibují vysoký výdělek s potřebou prakticky nulových zkušeností. Často navíc v inzerátu

úplně chybí zmínka o konkrétní náplni práce.

„Chcete si vydělat 70 tisíc Kč měsíčně a ještě se naučit s kryptoměnami?" stojí v titulku podvodné nabídky.

Pokud se osoby těmito podezřelými nabídkami nechají přesto zlákat, stávají se takzvanými „money mules" neboli bílými koňmi internetu. Podle Petra Baráka, experta na finanční bezpečnost České bankovní asociace (ČBA), jde o osoby, které si pachatelé najímají k legalizaci výnosů z páchané trestné činnosti.

„Hlavním úkolem ‚bílých koňů' je zamezit možnosti zpětného vypátrání pachatele podle finančního toku peněz. Oni sami neznají osoby, kterým peníze dál předávají, a jen ‚slepě' plní to, jak byli instruováni, tedy například vyzvednou peníze ze svého účtu v hotovosti a někomu je fyzicky předají nebo je vloží do kryptoměnového ATM (*bankomatu, pozn. red.*) nebo odešlou cestou anonymního převodu např. přes WesternUnion dle obdržené SMS/emailové instrukce," vysvětluje.

> Majitel firmy takto přišel o všechny firemní

> majitel firmy takto přišel všemi firemními peníze a neměl ani na výplaty svých zaměstnanců.
>
> PETR BARTÁK, EXPERT NA FINANČNÍ BEZPEČNOST ČBA

Za to si pak podle jeho slov sami rovnou odečtou odměnu z jimi převedené částky, která bývá většinou do 10 procent z její výše.

„Tuto činnost často provádějí, aniž by si uvědomovali, že jsou zneužiti k legalizaci výnosů pocházejících z trestné činnosti. Vidí jen možnost rychlého výdělku, který je jim nabídnut za pomoc, která je po nich žádána. Například ve formě smlouvy o provedení činnosti, brigády, pracovní smlouvy apod.," dodává expert.

To je důvod, proč se skupiny podvodníků zaměřují primárně na studenty, přistěhovalce nebo lidi v ekonomické tísni, kterým nabízejí snadný výdělek prostřednictvím legitimně vypadajících pracovních inzerátů a příspěvků na sociálních sítích.

Kampaň #nePINdej!

- Patří k nejrozsáhlejším kampaním v oblasti kyberbezpečnosti u nás. Zapojily se jak orgány státní správy, tak klíčové firmy českého byznysu, jichž samotných nebo jejich klientů se podvodné útoky také týkají.
- Kromě ČBA a Policie České republiky i Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), itego, a. s., Cisco, Thein Security, Česká pošta, ČEZ, Mastercard, O2 a České dráhy.
- Mediálními partnery jsou Česká televize (hlavní mediální partner), Seznam Zprávy, Deník a CineStar.

Investice nebo seznamka

Podvodníci lákají ale také například na výhodnost investování do kryptoaktiv. Právě na tento podvod se nechal zlákat majitel jedné firmy (redakce jeho totožnost zná, přál si zůstat v anonymitě) a umožnil přístup ke svému firemnímu účtu přes tzv. „vzdálenou plochu“ pachatelům. V tomto případě falešným investičním poradcům, kteří mu následně během několika minut z firemního účtu odcizili několik milionů korun, které rozeslali na účty bílých koní v různých bankách v Česku. Odtud pak tyto peníze s jejich pomocí odčerpali.

„To, že majitel firmy takto přišel o všechny firemní peníze a neměl ani na výplaty svých zaměstnanců, byla pak již jen smutná dohra celého případu, promítající se i do osudů dalších osob, na které jeho ‚neobezřetnost‘ rovněž dopadla,“ komentuje Petr Barták.

Falešný e-mail nebo odkaz v SMS. Podvod stojí jednoho člověka desetitisíce

13. 10. 17:38

Jiné jsou pak stále existující případy takzvaného „romance fraudu“, tedy internetových nabídek k seznámení se s údajným důstojníkem americké armády, lékařem pracujícím v Africe, osamoceným pracovníkem vrtné plošiny nebo dědicem majetku po bohatém strýčkovi, které byť existují už leta, stále nacházejí své oběti mezi klienty bank.

„Výsledkem jsou pak vědomé převody klientů mnohdy i statisícových částek podvodníkům vydávajícím se za takovéto osoby, na jejich zahraniční účty,“ dodává odborník na finanční bezpečnost.

Jak se nestát bílým koněm?

1. Reagujte jen na seriózní inzeráty. Nabídka rychlého, snadného a vysokého přivýdělku je vždy lákavá, ale ne nadarmo se říká, že bez práce nejsou koláče.
2. Nikdy nikomu nedávejte k dispozici svůj běžný účet pro převod peněz. Váš účet je jen váš a není důvod, aby ho někdo cizí využíval pro podezřelé transakce.
3. Nereagujte na inzeráty psané špatnou češtinou nebo s gramatickými či pravopisnými chybami. Pokud máte podezření na podvodné nabídky práce, kontaktujte Policii ČR.
4. Obdržíte-li na svůj účet peníze, které nečekáte a/nebo jsou od neznámé osoby, raději obratem kontaktujte svoji banku a transakci nahlaste. Nereagujte na výzvu odesílatele, ať částku přepošlete na jiný, jím uvedený účet. Dopustili byste se trestné činnosti.

Zdroj: Česká bankovní asociace, Kybertest

Počet obětí roste

A podle experta z ČBA navíc počet obětí, které se stávají bílými koňmi, dlouhodobě roste.

„Napomáhá tomu výrazně i současná ekonomická a geopolitická situace. Současně je od doby covidu i stále na vzestupu kybernetická kriminalita, a tedy i poptávka po těchto osobách ze strany pachatelů," vysvětluje.

A v příštích letech se situace jen tak nezlepší, spíše naopak. Barták totiž v budoucnosti očekává, že podvodů podobného charakteru bude ještě přibývat.

„Pachatelé si jsou velice dobře vědomi toho, že jejich vypátrání a dopadení ve virtuálním světě je mnohem složitější než v tom reálném," vysvětluje.

Co dokážou podvodné wifi. Stačilo projít kolem a data byla pryč

11. 12. 20:21

„Bude stále navíc existovat velký počet osob, které se nechají napálit kybernetickými podvody, a to nejen z ekonomických důvodů, ale i z důvodu, že budou přesvědčení o tom, že jich se tento typ podvodu netýká," tvrdí Barták.

„Pachatelé se za poslední dva roky takříkajíc ‚namlsali', tedy jejich úspěch (zisk) je bude o to více motivovat v pokračování v páchání tohoto typu trestné činnosti," uzavírá Petr Barták.

Seznam Zprávy jsou mediálním partnerem **kampaně #nePINdej.**

SDÍLEJTE ČLÁNEK

148. Vynalézaví podvodníci a důvěřiví lidé

Online ● praha7.cz (Regionální zprávy) ● 21. 12. 2022, 13:23

Autor: **Natalie Kolláriková** ● Rubrika: **Hobulet**

Dosah: 1 682 ● GRP: 0.02 ● OTS: 0.00 ● AVE: 7018.41 Kč

Odkaz: https://www.praha7.cz/vynalezavi-podvodnici-a-duverivi-lide/

PRAHA 7 Občan Organizace Volný čas Radnice Hledat Přihlášení Odběr novinek Kontakt Foreigners

Praha 7 \ Hobulet \ Prosinec 2022 \ Vynalézaví podvodníci a důvěřiví lidé

Vynalézaví podvodníci a důvěřiví lidé

Více než polovina Čechů se podle České bankovní asociace (ČBA) stala obětí hackerského útoku, a to bez ohledu na jeho dokončení. Třetina pak zná někoho, kdo byl obětí dokončeného útoku. Častá reakce po zaslechnutí zprávy o podvedených z našeho okolí bývá v mírně přezíravém tónu, protože máme dojem, že nám by se to určitě nestalo. Podvody, které slibují výhru nového iphonu, nebo gramaticky nepříliš správný e-mail o srdceryvném příběhu nigerijského prince, jenž potřebuje vaši pomoc, aby se dostal ke svému dědictví, už jsou ale minulostí. Současní podvodníci totiž bývají sofistikovanější.

– Text
Natalie Kolláriková
zdroj: Kybertest.cz a Česká bankovní asociace

– Ilustrace
Ondřej Basjuk
(*1983) je domažlický rodák, malíř a grafik, který vystudoval Fakultu designu a umění v Plzni a Akademii výtvarných umění v Praze. Vystavoval v pražské Galerii Jelení, Galerii KIN Jídelna, Entrance Gallery nebo v brněnské Fait Gallery. Je zastoupen v prestižních sbírkách v České republice i v zahraničí.

– Publikováno 21. 12. 2022
– Upraveno 21. 12. 2022

S hackerským útokem se nejčastěji setkávají lidé mezi 18 a 34 lety. V roce 2022 se s útokem setkalo 27 % Čechů. Podle České bankovní asociace se počet útoků za

poslední dva roky zvýšil čtyřnásobně a průměrná škoda u dokončeného útoku je na jednoho klienta 162 tisíc korun. Útočníci nejčastěji cílí na získání přihlašovacích údajů, a to ve 40 % případů. Téměř třetina se pak snažila získat číslo platební karty a čtvrtina se zaměřila na osobní údaje, jako je například rodné číslo. Zájem byl také o heslo nebo PIN, a to ve 22 % případů.

Česká bankovní asociace (ČBA) ve spolupráci se svými partnery minulé září spustila celonárodní kampaň NePINdej, na jejíchž stránkách kybertest.cz si můžete ověřit své znalosti základních principů bezpečného chování na internetu. Po dvou měsících od spuštění kampaň přilákala téměř 54 tisíc lidí, kteří testem prošli v průměru se 70% úspěšností. Nejčastější typy podvodů už nejsou pouze po e-mailech nebo SMS, ale v poslední době se jedná také o telefonní hovory a podvodný prodej přes inzertní servery. ČBA nedávno spustila i obdobu Kybertestu pro mladší generaci. Kyberhra.cz cílí na žáky druhého stupně základních a středních škol, odborných učilišť a víceletých gymnázií. Mladiství jsou totiž snadným cílem. V kyberprostoru se pohybují velmi často, ale přesně nevědí, jak se v on-line prostředí bezpečně chovat.

Připomeňme si nejčastější typy podvodů a jednoduché rady, jak se podvodníkům ubránit.

Phishing
Podvodná technika používaná k získávání citlivých údajů v elektronické komunikaci se označuje phishing. Cílem těchto útoků je získání vašich citlivých údajů, například čísla platební karty, nebo stažení škodlivého softwaru do vašeho zařízení. Je nutné si uvědomit, že kupříkladu vaše banka by prostřednictvím e-mailu citlivé údaje nebo heslo do internetového bankovnictví nikdy nepožadovala. Dalším druhem phishingových e-mailů je předstírání známé autority – finančního nebo generálního ředitele nějaké společnosti s naléhavou potřebou uhradit fakturu nebo převést peníze. Podvodníci tohoto typu mají pečlivě nastudované detaily, a dokážou tak velmi autenticky předstírat, že jsou danou důvěryhodnou osobou.

Phishing útočí i prostřednictvím sociálních sítí. Nejčastější podobou je proniknutí do profilu a následné rozesílání zpráv s podvrženým odkazem přátelům. Útočník často ani nemusí do profilu proniknout, ale jednoduše napadený profil zkopíruje a lidem z adresáře odešle zprávu, která vypadá, jako kdyby byla odeslaná z pravého profilu. Zpráva často obsahuje žádost o peníze nebo podvodné linky, jejichž cílem je opět snaha získat citlivé údaje.

Zkontrolujte jméno a e-mailovou adresu odesílatele. E-mailová doména odesílatele by měla být shodná s názvem obchodní společnosti odesílatele e-mailu. To platí i pro název domény (to, co následuje po @). Na první pohled může vypadat v pořádku, ale ve skutečnosti může být překroucená, jinak napsaná.

Odpověď na e-mail může být totiž odeslána příjemci odlišnému od odesílatele. Tuto informaci najdete v detailech e-mailu pod odesílatelem jako „Reply-to“ neboli „Odpovědět na“. Pokud je to tak, ověřte i tuto adresu. Jinak mohou informace, které v odpovědi odešlete, skončit u podvodníka.

Zaměřte se na obsah a gramatiku. Pokud zpráva obsahuje neobvyklé fráze nebo gramatické chyby, může se jednat o podvodný e-mail.

Dejte si pozor na časový nátlak. Podvodný e-mail se často snaží navodit dojem, že je potřeba vykonat něco okamžitě, protože například došlo k zablokování bankovního účtu nebo je třeba obratem uhradit fakturu, jinak spadnete do exekuce.

Věnujte pozornost odkazům a přílohám. Pokud jsou v e-mailu nebo ve zprávě na sociálních sítích odkazy a přílohy, musíte být opatrní. Často vás zprávy můžou přesvědčovat, abyste klikli na odkaz nebo stáhli a otevřeli přílohu. Tyto přílohy však mohou sloužit k maskování virů nebo malwaru, které po stažení nebo otevření mohou vést buď ke ztrátě osobních údajů, nebo k instalaci škodlivého softwaru do počítače nebo telefonu. Pozor také na zrádné ikonky, tlačítka a obrázky, odkazy mohou být skryté právě pod nimi.

Webová adresa by měla být vždy shodná s oficiálním webem odesílatele. Předtím než kliknete na ikonku, najeďte na ni myší. Kompletní cílový odkaz se vám pak zobrazí v levém dolním rohu e-mailové aplikace nebo jako tip vedle kurzoru myši.

Smishing
Podvodných SMS v poslední době také značně přibývá. Velmi často se jedná o zprávy, které vypadají, jako by je zaslala některá z doručovacích společností nebo vaše banka. Úspěšnost podvodu je závislá nejen na kvalitě provedení, ale i na načasování – před Vánocemi nebo v období daňových přiznání. Odhalit podvodnou SMS přitom nemusí být tak jednoduché, jak se na první pohled zdá. Podvodníci totiž dokážou napodobit prakticky jakéhokoliv odesílatele zprávy a ta se vám tak může dokonce automaticky přiřadit do vlákna předchozí komunikace s daným subjektem. I v rámci podvodu přes SMS, tzv. smishingu, je dobré znát několik pravidel.

Pokud si pravostí zprávy nejste jistí, nereagujte na ni, zvláště pokud jde o výzvy k blokaci internetového bankovnictví nebo třeba zaplacení nedoplatku daně.

Nikdy si na základě výzvy nestahujte do telefonu aplikace a neklikejte na odkazy.

Pokud obdržíte SMS o doručení zásilky, ověřte si, zda nějakou zásilku opravdu očekáváte, a to na oficiálních stránkách přepravce nebo doručovací služby.

Vishing
Další úrovní jsou podvodné telefonáty – vishing – od údajných bankéřů, policistů nebo investičních poradců. Tento způsob je o to zákeřnější, že se jedná o telefonní hovor s živým člověkem. Podvodník se představí jako pracovník banky, policista, lékař aj. a na hovor se velmi dobře připraví – bude znát vaše jméno a adresu i číslo vašeho bankovního účtu. Pod záminkou napadení vašeho účtu, pomoci zraněnému příbuznému či ochrany vašich peněz po vás bude opětovně chtít různé přihlašovací a citlivé údaje nebo potvrzovací SMS, jejímž cílem není nic jiného než vás připravit o peníze. Před dvěma lety se počet vishingových podvodů pohyboval v nízkých stovkách, letos mluvíme již o desítkách tisíc. A narostla i jejich úspěšnost. „Téměř každý druhý podvodný telefonát v současné době bohužel skončí škodou pro klienta. Průměrná částka, o kterou klienti při těchto útocích přijdou, je ale přitom dost vysoká, zhruba čtvrt milionu korun," podotýká Monika Zahálková, výkonná ředitelka České bankovní asociace.

Mějte na paměti, že zaměstnanec banky nebo policista po vás nikdy nebude chtít citlivé údaje, protože je nepotřebuje.

Pokud máte jakékoliv pochybnosti o pravosti hovoru, zavěste. Na oficiálních stránkách instituce, za jejíhož zaměstnance se podvodník vydával, vyhledejte telefonní číslo na infolinku a instituci kontaktujte. Nikdy nevolejte zpět na číslo útočníka.

M-platba
Mobilní platba (m-platba) funguje podobně jako platba platební kartou, avšak na rozdíl od placení kartou vám nejsou peníze strženy z účtu, nýbrž z vašeho předplaceného kreditu nebo měsíčního tarifu u mobilního operátora. Mobilní platbou je možné hradit různé on-line nákupy, třeba nákup jízdenek MHD nebo nákupy

spojené s herním průmyslem. Při využití m-platby nemusíte prodejci poskytovat údaje o své platební kartě, ale nákup potvrdíte jednorázovým kódem, který vám operátor zašle v SMS.

Cílem podvodníka je získat vaše telefonní číslo. Získané číslo pak podvodník zadá do platební brány a zvolí způsob úhrady prostřednictvím m-platby. Provozovatel platební brány ale potřebuje ještě platbu verifikovat ověřovacím kódem. Automaticky pak odesílá na uvedené – tedy vaše – telefonní číslo SMS s kódem. Podvodník od vás tento kód bude chtít získat, což mu umožní realizovat m-platbu, a strhnout tak peníze z vašeho účtu.

Profily na sociálních sítích mějte zabezpečené dvoufázovým ověřením. Pokud by pachatel získal vaše přihlašovací údaje, musel by z vás vylákat ještě i autorizační kód. V případě, že vám někdo profil na sociální síti napadl, ihned kontaktujte zákaznickou podporu sociální sítě a okamžitě si změňte heslo.

Na sociální sítě, do e-mailových profilů, do on-line bankovnictví apod. se přihlašujte pouze z oficiálních webových stránek.

Nikdy nikomu nesdělujte žádné kódy, které jste obdrželi, ať již v SMS, nebo jiným způsobem.

Nečekaný podraz

Prodávali jste někdy něco na inzertních serverech? Potom si mohli podvodníci vyhlédnout i vás a vylákat z vás podvodem peníze. Přesto, že se jedná o celkem nový druh podvodu, setkáváme se s ním stále častěji. Podvodníci získají z inzerátu vaši e-mailovou adresu nebo telefonní číslo a kontaktují vás prostřednictvím aplikací WhatsApp nebo Messenger s předstíraným zájmem o koupi inzerovaného zboží. Během konverzace vás naváději k tomu, abyste uhradili poplatek za přepravu zboží, kterou kupující (tedy podvodník) zajistí, a to přes platební bránu jimi domluveného dopravce. V odkazu na falešnou platební bránu, který vám ve zprávě zašlou, po vás chtějí vyplnit citlivé údaje o platební kartě včetně PIN, případně přístupové údaje do on-line bankovnictví včetně hesla a bezpečnostního kódu z autorizační SMS. Díky získaným údajům se podvodník dostane do vašeho on-line bankovnictví, kde provede převod finančních prostředků na svůj bankovní účet, nebo na základě zjištěných údajů z platební karty provede její tokenizaci (tokenizace platby je proces nahrazení tradičního čísla platební karty unikátním tokenem, pozn. red.) a následně v bezkontaktním bankomatu vybere z vašeho účtu peníze. „Protože jsou prodávající klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se od nich někdo snaží získat přístupové údaje k účtům nebo do jejich internetového bankovnictví. Aby co nejdříve docílili prodeje zboží, neopatrně spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatně. Opak je bohužel pravdou, většinou o všechno přijdou," objasňuje pplk. Ondřej Kapr z Policie ČR.

Pokud na inzerát reaguje cizinec, zbystřete.

Buďte na pozoru, když kupující požaduje nestandardní způsob dopravy nebo způsob platby. Příkladem je zajištění jeho platby „přepravní společností", která peníze uvolní, až bude zboží na cestě, nebo platební brána, která vyžaduje údaje z platební karty prodávajícího.

Nereagujte na požadavky kupujícího, že zaplatí přes neznámé služby různých nebankovních platebních společností nebo v kryptoměně. Nepřistupujte na platbu nedoplatků, přeplatků či kaucí.

Lstivé aplikace
Jedním z velmi aktuálních triků útočníků jsou i infikované mobilní aplikace či jejich aktualizace, které si nejčastěji stáhnete z neoficiálních obchodů s aplikacemi a webových stránek. Výjimkou ale nejsou ani podvodné aplikace nainstalované přímo z oficiálního obchodu. Pokud v telefonu nemáte nainstalovaný bezpečnostní software, který by vás varoval, a při instalaci aplikaci udělíte vysoká oprávnění – například aplikaci pro nahrávání hovorů i přístup k fotoaparátu či SMS – dokáže aplikace odcizit vaše přihlašovací údaje do bankovnictví, obejít dvoufázové ověření či získat potvrzovací SMS.

Stahujte aplikace jen z důvěryhodných zdrojů – nejlépe Google Play či App Store. Před stažením věnujte pozornost recenzím a hodnocení aplikace a tomu, zda nejste mezi prvními, kdo aplikaci stahuje. Ověřte si i jméno vývojáře a to, zda vyvinul více aplikací.

Při udělování oprávnění aplikacím se řiďte heslem, že méně je někdy více. Dobře si rozmyslete, zda stahovaná aplikace opravdu potřebuje přístup k vašim fotkám, kontaktům, úložišti, poloze apod.

Klamný e-shop
Určitě máte zkušenost s nakupováním v některém z osvědčených e-shopů. Je to pohodlné, přehledné, jednoduché a rychlé a často jsou zde ceny nižší než v kamenných obchodech. Avšak i zde můžete při nedostatečné pozornosti snadno naletět podvodníkům. Stačí, abyste přes odkaz na „výhodný“ nákup zboží v on-line reklamě nebo v nevyžádaném e-mailu navštívili inzerovaný e-shop a nakoupili. Pokud si obchod předem neprověříte, můžete přijít o peníze, citlivé údaje a buď žádné zboží nakonec neobdržíte, nebo obdržíte, ale bude pochybné kvality.

Než někam vyplníte přístupové údaje či hesla, vždy si zkontrolujte webovou adresu. Webová adresa by měla být shodná s tou, kterou instituce uvádí ve všech kontaktních informacích.

Zkontrolujte si, zda e-shop či webová stránka uvádějí kontaktní údaje a v jaké formě. Zbystřete, pokud je na stránkách pouze kontaktní formulář nebo obsahuje-li stránka pravopisné chyby a překlepy.

Podle zákona musí být na webových stránkách obchodu na viditelném místě umístěny obchodní podmínky.

Ověřte si existenci e-shopu – např. na stránkách Justice.cz nebo u ČOI, která také provozuje databázi podvodných a rizikových e-shopů – www.coi.cz/pro-spotrebitele/rizikove-e-shopy. Také si vyhledejte recenze – pokud žádné nenajdete nebo najdete pouze negativní, mějte se na pozoru.

Podezřelá wi-fi
Vaše mobilní zařízení v sobě uchovává mnoho citlivých údajů. Od fotografií přes kontaktní údaje, hesla až po přístupy do on-line bankovnictví. To všechno jsou přesně informace, které podvodníky zajímají. Doma nebo v práci či ve škole jste připojeni přes zabezpečenou wi-fi síť. Co ale třeba v obchodním centru nebo v hotelu? Tam všude je vám k dispozici veřejná wi-fi síť, která má ale většinou slabé zabezpečení

a může být velice snadno zneužita podvodníky. Připojení k takové síti může být pro vaše data nebezpečné. Věnujte pozornost názvu nabízené veřejné wi-fi sítě. Pokud se jmenuje třeba Public Pardubice, ale vy v Pardubicích nejste, je to podezřelé.

Jakmile je u veřejné wi-fi znak otevřeného zámečku, mějte na paměti, že vaši komunikaci může kdokoli „odposlouchávat".

Nepovolujte automatické připojování k neznámým wi-fi sítím.

Pro zvýšení své bezpečnosti používejte VPN – virtuální privátní síť.

Pokud si nejste jisti zabezpečením používané wi-fi sítě, nezadávejte nikam své citlivé údaje. Za připojení k veřejné wi-fi síti nikdy nic neplaťte.

ZÁKLADNÍ DESATERO BEZPEČNOSTI

Starejte se o bezpečí svého počítače Nainstalujte a pravidelně aktualizujte antiviry a firewally na svém počítači na nejnovější verzi. Zvýšíte tak bezpečnost svých souborů.

Zabezpečte si mobilní telefon Určitě se do svých účtů přihlašujete častěji ze svého smartphonu než z počítače, chráníte ho ale minimálně stejně? V každém mobilním obchodě s aplikacemi najdete mnoho bezpečnostních aplikací, které jsou dostupné zdarma nebo za malý poplatek.

Ověřujte si původ aplikací Aplikace a programy stahujte vždy z důvěryhodných a ověřených zdrojů, nejlépe přímo z oficiálních internetových obchodů s mobilními aplikacemi (Google Play či App Store). Před stažením věnujte aplikaci pozornost – čtěte recenze, zaměřte se na hodnocení a nebuďte mezi prvními, kdo ji stahuje.

Chraňte své přihlašovací údaje Se svými přihlašovacími a osobními údaji zacházejte opatrně. Nikomu je nesdělujte a neukládejte je na počítačích ve veřejných sítích nebo ve škole. Myslete na to, že banka vaše přihlašovací údaje nikdy nežádá a už vůbec ne telefonicky, e-mailem anebo prostřednictvím sociálních sítí.

PIN jako oko v hlavě Je váš PIN datum narození nebo 1234? Rychle si ho změňte a zapamatujte. Pokud víte, že jste zapomnětliví a musíte si PIN zapsat, nenechávejte ho v blízkosti platební karty a střežte ho jako oko v hlavě. Mějte bezpečné heslo Heslo by mělo být neodhadnutelné (ne vaše jméno apod.), silné (kombinace

velkých i malých písmen a znaků), nezjistitelné (př. hackerský program zkouší slova ze slovníku) a především unikátní –
nikdy nepoužívejte stejné heslo pro různé služby (sociální sítě, e-mail a bankovní účet). Hesla s nikým nesdílejte a neukládejte je do prohlížeče. Pokud si je nezapamatujete, zapište si je, ale následně uložte na bezpečné místo. Pokud je to možné, zvolte k účtům dvoufaktorové ověřování.

Pozor na neznámé přílohy Neotvírejte e-maily ani přílohy od neznámých a podezřelých odesílatelů, neklikejte ani na žádné odkazy v těle těchto e-mailů. Vždy raději zkontrolujte e-mailovou adresu odesílatele a pravopis.

Nakupujte jen u prověřených on-line prodejců Přes internet nakupujte jen u prověřených a důvěryhodných prodejců – orientujte se podle ikony zamknutého visacího zámku u URL adres jejich webu, musí být bez jakéhokoli upozornění. To samé platí u přihlašování na jakýkoli web, bank zejména. U soukromých inzerentů a méně známých prodejců čtěte recenze.

Čtěte upozornění banky Nejen ta bankovní, ale také vašeho počítače. Pokud upozornění jen odkliknete, může vám např. uniknout zpráva z vaší banky o útocích hackerů. Věnujte jim pozornost a chraňte sebe i svůj účet.

Informujte banku Pokud máte byť jen podezření, že se s vaším účtem děje něco podivného či špatného, kontaktujte svou banku. Přes infolinku vám zákaznická podpora dokáže zkontrolovat váš účet a případně zablokovat příkazy.

149. Vynalézaví podvodníci a důvěřiví lidé

Tisk ● Hobulet (Praha 7); str. 6, 7 (Regionální zprávy) ● 21. 12. 2022

Vydavatel: **Městská část Praha 7 (cz-00063754)** ● Autor: **Natalie Kolláriková** ● Rubrika: **Téma**

Dosah: 30 000 ● GRP: 0.33 ● OTS: 0.00 ● AVE: 62000.00 Kč

Odkaz: náhled

Vynalézaví podvodníci a důvěřiví lidé

Více než polovina Čechů se podle České bankovní asociace (ČBA) stala obětí hackerského útoku, a to bez ohledu na jeho dokončení. Třetina pak zná někoho, kdo byl obětí dokončeného útoku. Častá reakce po zaslechnutí zprávy o podvedených z našeho okolí bývá v mírně přezíravém tónu, protože máme dojem, že nám by se to určitě nestalo. Podvody, které slibují výhru nového iphonu, nebo gramaticky nepřílišsprávný e-mail o srdceryvném příběhu nigerijského prince, jenž potřebuje vaši pomoc, aby se dostal ke svému dědictví, už jsou ale minulostí. Současní podvodníci totiž bývají sofistikovanější.

S hackerským útokem se nejčastěji setkávají lidé mezi 18 a 34 lety. V roce 2022 se s útokem setkalo 27 % Čechů. Podle České bankovní asociace se počet útoků za poslední dva roky zvýšil čtyřnásobně a průměrná škoda u dokončeného útoku je na jednoho klienta 162 tisíc korun. Útočníci nejčastěji cílí na získání přihlašovacích údajů, a to ve 40 % případů. Téměř třetina se pak snažila získat číslo platební karty a čtvrtina se zaměřila na osobní údaje, jako je například rodné číslo. Zájem byl také o heslo nebo PIN, a to ve 22 % případů.

Česká bankovní asociace (ČBA) ve spolupráci se svými partnery minulé září spustila celonárodní kampaň NePINdej, na jejíchž stránkách kybertest.cz si můžete ověřit své znalosti základních principů bezpečného chování na internetu. Po dvou měsících od spuštění kampaň přilákala téměř 54 tisíc lidí, kteří testem prošli v průměru se 70% úspěšností. Nejčastější typy podvodů už nejsou pouze po e-mailech nebo SMS, ale v poslední době se jedná také o telefonní hovory a podvodný prodej přes inzertní servery. ČBA nedávno spustila i obdobnou Kybertestu pro mladší generaci. Kyberhra.cz cílí na žáky druhého stupně základních a středních škol, odborných učilišť a víceletých gymnázií. Mladiství jsou totiž snadným cílem. V kyberprostoru se pohybují velmi často, ale přesně nevědí, jak se v on-line prostředí bezpečně chovat.

Připomeňme si nejčastější typy podvodů a jednoduché rady, jak se podvodníkům ubránit.

Text – Natalie Kolláriková, zdroj: Kybertest.cz a Česká bankovní asociace
Ilustrace – Ondřej Basjuk

Phishing

Podvodná technika používaná k získávání citlivých údajů v elektronické komunikaci se označuje phishing. Cílem těchto útoků je získání vašich citlivých údajů, například čísla platební karty, nebo stažení škodlivého software do vašeho zařízení. Je nutné si uvědomit, že kupříkladu vaše banka by prostřednictvím e-mailu citlivé údaje nebo heslo do internetového bankovnictví nikdy nepožadovala.

Dalším druhem phishingových e-mailů je předstírání známé autority - finančního nebo generálního ředitele nějaké společnosti s naléhavou potřebou uhradit fakturu nebo převést peníze. Podvodníci tohoto typu mají pečlivě nastudované detaily, a dokážou tak velmi autenticky předstírat, že jsou danou důvěryhodnou osobou.

Phishing útočí i prostřednictvím sociálních sítí. Nejčastější podobou je pronikнutí do profilu a následné rozesílání zpráv s podvrženým odkazem přátelům. Útočník často ani nemusí do profilu proniknout, ale jednoduše napadený profil zkopíruje a lidem z adresáře odešle zprávu, která vypadá, jako kdyby byla odeslaná z pravého profilu. Zpráva často obsahuje žádost o peníze nebo podvodné linky, jejichž cílem je opět snaha získat citlivé údaje.

Zkontrolujte jméno a e-mailovou adresu odesílatele. E-mailová doména odesílatele by měla být shodná s názvem obchodní společnosti odesílatele e-mailu. To platí i pro název domény (to, co následuje po @). Na první pohled může vypadat v pořádku, ale ve skutečnosti může být překroucená, jinak napsaná.

Odpověď na e-mail může být totiž odeslána příjemci odlišnému od odesílatele. Tuto informaci najdete v detailech e-mailu pod odesílatelem jako „Reply-to" neboli „Odpovědět na". Pokud je to tak, ověřte i tuto adresu. Jinak mohou informace, které v odpovědi odešlete, skončit u podvodníka.

Zaměřte se na obsah a gramatiku. Pokud zpráva obsahuje neobvyklé fráze nebo gramatické chyby, může se jednat o podvodný e-mail.

Dejte si pozor na časový nátlak. Podvodný e-mail se často snaží navodit dojem, že je potřeba vykonat něco okamžitě, protože například došlo k zablokování bankovního účtu nebo je třeba obratem uhradit fakturu, jinak spadnete do exekuce.

Věnujte pozornost odkazům a přílohám. Pokud jsou v e-mailu nebo ve zprávě na sociálních sítích odkazy a přílohy, musíte být opatrní. Často vás zprávy můžou přesvědčovat, abyste klikli na odkaz nebo stáhli a otevřeli přílohu. Tyto přílohy však mohou sloužit k maskování virů nebo malwaru, které po stažení nebo otevření mohou vést buď ke ztrátě osobních údajů, nebo k instalaci škodlivého softwaru do počítače nebo telefonu. Pozor také na zrádné ikonky, tlačítka a obrázky, odkazy mohou být skryté právě pod nimi.

Webová adresa by měla být vždy shodná s oficiálním webem odesílatele. Předtím než kliknete na ikonku, najeďte na ni myší. Kompletní cílový odkaz se vám pak zobrazí v levém dolním rohu e-mailové aplikace nebo jako tip vedle kurzoru myši.

Smishing

Podvodných SMS v poslední době také značně přibývá. Velmi často se jedná o zprávy, které vypadají, jako by je zaslala některá z doručovacích společností nebo vaše banka. Úspěšnost podvodu je závislá nejen na kvalitě provedení, ale i na načasování - před Vánocemi nebo v období daňových přiznání. Odhalit podvodnou SMS přitom nemusí být tak jednoduché, jak se na první pohled zdá. Podvodníci totiž dokážou napodobit prakticky jakéhokoliv odeslatele zprávy a ta se vám tak může dokonce automaticky přiřadit do vlákna předchozí komunikace s daným subjektem. I v rámci podvodu přes SMS, tzv. smishingu, je dobré znát několik pravidel.

Pokud si pravostí zprávy nejste jisti, nereagujte na ni, zvláště pokud jde o výzvy k blokaci internetového bankovnictví nebo třeba zaplacení nedoplatku daně.

Nikdy si na základě výzvy nestahujte do telefonu aplikace a neklikejte na odkazy.

Pokud obdržíte SMS o doručení zásilky, ověřte si, zda nějakou zásilku opravdu očekáváte, a to na oficiálních stránkách přepravce nebo doručovací služby.

Vishing

Další úrovní jsou podvodné telefonáty - vishing - od údajných bankéřů, policistů nebo investičních poradců. Tento způsob je o to zákeřnější, že se jedná o telefonní hovor s živým člověkem. Podvodník se představí jako pracovník banky, policista, lékař aj. a na hovor se velmi dobře připraví - bude znát vaše jméno a adresu i číslo vašeho bankovního účtu. Pod záminkou napadení vašeho účtu, pomoci zraněnému příbuznému či ochrany vašich peněz po vás bude opětovně chtít různé přihlašovací a citlivé údaje nebo potvrzovací SMS, jejímž cílem není nic jiného než vás připravit o peníze. Před dvěma lety se počet vishingových podvodů pohyboval v nízkých stovkách, letos mluvíme již o desítkách tisíc. A narostla i jejich úspěšnost. „Téměř každý druhý podvodný telefonát v současné době bohužel skončí škodou pro klienta. Průměrná částka, o kterou klienti při těchto útocích přijdou, je ale přitom dost vysoká, zhruba čtvrt miliónu korun," podotýká Monika Zahálková, výkonná ředitelka České bankovní asociace.

Mějte na paměti, že zaměstnanec banky nebo policista po vás nikdy nebude chtít citlivé údaje, protože je nepotřebuje.

Pokud máte jakékoliv pochybnosti o pravosti hovoru, zavěste. Na oficiálních stránkách instituce, za jejíhož zaměstnance se podvodník vydával, vyhledejte telefonní číslo na infolinku a instituci kontaktujte. Nikdy nevolejte zpět na číslo útočníka.

M-platba

Mobilní platba (m-platba) funguje podobně jako platba platební kartou, avšak na rozdíl od placení kartou vám nejsou peníze strženy z účtu, nýbrž z vašeho předplaceného kreditu nebo měsíčního tarifu u mobilního operátora. Mobilní platbou je možné hradit různé on-line nákupy, třeba nákup jízdenek MHD nebo nákupy spojené s hrním průmyslem. Při využití m-platby nemusíte prodejci poskytovat údaje o své platební kartě, ale nákup potvrdíte jednorázovým kódem, který vám operátor zašle v SMS.

Cílem podvodníka je získat vaše telefonní číslo. Získané číslo pak podvodník zadá do platební brány a zvolí způsob úhrady prostřednictvím m-platby. Provozovatel platební brány ale potřebuje ještě platbu verifikovat ověřovacím kódem. Automaticky pak odešlá na uvedené - tedy vaše - telefonní číslo SMS s kódem. Podvodník od vás tento kód bude chtít získat, což mu umožní realizovat m-platbu, a strhnout tak peníze z vašeho účtu.

Profily na sociálních sítích mějte zabezpečené dvoufázovým ověřením. Pokud by pachatel získal vaše přihlašovací údaje, musel by z vás vylákat ještě i autorizační kód. V případě, že vám někdo profil na sociální síti napadl, ihned kontaktujte zákaznickou podporu sociální sítě a okamžitě si změňte heslo.

Na sociální sítě, do e-mailových profilů, do on-line bankovnictví apod. se přihlašujte pouze z oficiálních webových stránek.

Nikdy nikomu nesdělujte žádné kódy, které jste obdrželi, ať již v SMS, nebo jiným způsobem.

Nečekaný podraz

Prodávali jste někdy něco na inzertních serverech? Potom si mohli podvodníci vyhlédnout i vás a vylákat z vás podvodem peníze. Přesto, že se jedná o celkem nový druh podvodu, setkáváme se s ním stále častěji. Podvodníci získají z inzerátu vaši e-mailovou adresu nebo telefonní číslo a kontaktují vás prostřednictvím aplikací WhatsApp nebo Messenger s představeným zájmem o koupi inzerovaného zboží. Během konverzace vás navádějí k tomu, abyste uhradili poplatek za přepravu zboží, kterou kupující (tedy podvodníci) zajistí, a to přes platební bránu jimi domluveného dopravce. V odkazu na falešnou platební bránu, který vám ve zprávě zašlou, po vás chtějí vyplnit citlivé údaje o platební kartě včetně PIN, případně přístupové údaje do on-line bankovnictví včetně hesla a bezpečnostního kódu z autorizační SMS. Díky získaným údajům se podvodník dostane do vašeho on-line bankovnictví, kde provede převod finančních prostředků na svůj bankovní účet, nebo na základě zjištěných údajů z platební karty provede její tokenizaci (tokenizace platby je proces nahrazení tradičního čísla platební karty unikátním tokenem, pozn. red.) a následně v bezkontaktním bankomatu vybere z vašeho účtu peníze. „Protože jsou prodávající klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se od nich někdo snaží získat přístupové údaje k účtům nebo do jejich internetového bankovnictví. Aby co nejdříve docílili prodeje zboží, neopatrně spolupracují a vyplňují údaje o svých kartách a přístupech na účet v domnění, že nedělají nic špatné. Opak je bohužel pravdou, většinou o všechno přijdou," objasňuje ppłk. Ondřej Kapr z Policie ČR.

Pokud na inzerát reaguje cizinec, zbystřete.

Buďte na pozoru, když kupující požaduje nestandardní způsob dopravy nebo způsob platby. Příkladem je zajištění jeho platby „přepravní společností", která peníze uvolní, až bude zboží na cestě, nebo platební brána, která vyžaduje údaje z platební karty prodávajícího.

Nereagujte na požadavky kupujícího, že zaplatí přes neznámé služby různých nebankovních platebních společností nebo v kryptoměně. Nepřistupujte na platbu nedoplatků, přeplatků či kauci.

Lstivé aplikace

Jedním z velmi aktuálních triků útočníků jsou i infikované mobilní aplikace či jejich aktualizace, které si nejčastěji stáhnete z neoficiálních obchodů s aplikacemi a webových stránek. Výjimkou ale nejsou ani podvodné aplikace nainstalované přímo z oficiálního obchodu. Pokud v telefonu nemáte nainstalovaný bezpečnostní software, který by vás varoval, a při instalaci aplikaci udělíte vysoká oprávnění - například aplikaci pro nahrávání hovorů i přístup k fotoaparátu či SMS - dokáže aplikace odcizit vaše přihlašovací údaje do bankovnictví, obejít dvoufázové ověření či získat potvrzovací SMS.

Stahujte aplikace jen z důvěryhodných zdrojů - nejlépe Google Play či App Store. Před stažením věnujte pozornost recenzím a hodnocení aplikace a tomu, zda nejste mezi prvními, kdo aplikaci stahuje. Ověřte si i jméno vývojáře a to, zda vyvinul více aplikací.

Při udělování oprávnění aplikacím se řiďte heslem, že méně je někdy více. Dobře si rozmyslete, zda stahovaná aplikace opravdu potřebuje přístup k vašim fotkám, kontaktům, úložišti, poloze apod.

Klamný e-shop

Určitě máte zkušenost s nakupováním v některém z osvědčených e-shopů. Je to pohodlné, přehledné, jednoduché a rychlé a často jsou zde ceny nižší než v kamenných obchodech. Avšak i zde můžete při nedostatečné pozornosti snadno naletět podvodníkům. Stačí, abyste přes odkaz na „výhodný" nákup zboží v on-line reklamě nebo v nevyžádaném e-mailu navštívili inzerovaný e-shop a nakoupili. Pokud si obchod předem neprověříte, můžete přijít o peníze, citlivé údaje a buď žádné zboží nakonec neobdržíte, nebo obdržíte, ale bude pochybné kvality.

Než někam vyplníte přístupové údaje či hesla, vždy si zkontrolujte webovou adresu. Webová adresa by měla být shodná s tou, kterou instituce uvádí ve všech kontaktních informacích. Zkontrolujte si, zda e-shop či webová stránka uvádějí kontaktní údaje a v jaké formě. Zbystřete, pokud je na stránkách pouze kontaktní formulář nebo obsahuje-li stránka pravopisné chyby a překlepy.

Podle zákona musí být na webových stránkách obchodu na viditelném místě umístěny obchodní podmínky.

Ověřte si existenci e-shopu - např. na stránkách Justice.cz nebo u ČOI, která také provozuje databázi podvodných a rizikových e-shopů - www.coi.cz/pro-spotrebitele/rizikove-e-shopy. Také si vyhledejte recenze - pokud žádné nenajdete nebo najdete pouze negativní, mějte se na pozoru.

Podezřelá wi-fi

Vaše mobilní zařízení v sobě uchovává mnoho citlivých údajů. Od fotografií přes kontaktní údaje, hesla až po přístupy do on-line bankovnictví. To všechno jsou přesně informace, které podvodníky zajímají. Doma nebo v práci či ve škole jste připojeni přes zabezpečenou wi-fi síť. Co ale třeba v obchodním centru nebo v hotelu? Tam všude je vám k dispozici veřejná wi-fi síť, která má ale většinou slabé zabezpečení a může být velice snadno zneužita podvodníky. Připojení k takové síti může být pro vaše data nebezpečné. Věnujte pozornost názvu nabízené veřejné wi-fi sítě. Pokud se jmenuje třeba Public Pardubice, ale vy v Pardubicích nejste, je to podezřelé.

Jakmile je u veřejné wi-fi znak otevřeného zámečku, mějte na paměti, že vaši komunikaci může kdokoli „odposlouchávat".

Nepovolujte automatické připojování k neznámým wi-fi sítím.

Pro zvýšení své bezpečnosti používejte VPN - virtuální privátní síť.

Pokud si nejste jisti zabezpečením používané wi-fi sítě, nezadávejte nikam své citlivé údaje. Za připojení k veřejné wi-fi sítí nikdy nic neplaťte. ⊕

ZÁKLADNÍ DESATERO BEZPEČNOSTI

Starejte se o bezpečí svého počítače Nainstalujte a pravidelně aktualizujte antiviry a firewally na svém počítači na nejnovější verzi. Zvýšíte tak bezpečnost svých souborů.

Zabezpečte si mobilní telefon Určitě se do svých účtů přihlašujete častěji ze svého smartphonu než z počítače, chraňte ho ale minimálně stejně! V každém mobilním obchodě s aplikacemi najdete mnoho bezpečnostních aplikací, které jsou dostupné zdarma nebo za malý poplatek.

Ověřujte si původ aplikací Aplikace a programy stahujte vždy z důvěryhodných a ověřených zdrojů, nejlépe přímo z oficiálních internetových obchodů s mobilními aplikacemi (Google Play či App Store). Před stažením věnujte aplikaci pozornost – čtěte recenze, zaměřte se na hodnocení a nebuďte mezi prvními, kdo ji stahuje.

Chraňte své přihlašovací údaje Se svými přihlašovacími a osobními údaji zacházejte opatrně. Nikomu je nesdělujte a neukládejte je na počítačích ve veřejných sítích nebo ve škole. Myslete na to, že banka vaše přihlašovací údaje nikdy nežádá a už vůbec ne telefonicky, e-mailem anebo prostřednictvím sociálních sítí.

PIN jako oko v hlavě Je váš PIN datum narození nebo 12345? Rychle si ho změňte a zapamatujte. Pokud víte, že jste zapomnětliví a musíte si PIN zapsat, nenechávejte ho v blízkosti platební karty a střežte ho jako oko v hlavě.

Mějte bezpečné heslo Heslo by mělo být neodhadnutelné (ne vaše jméno apod.), silné (kombinace velkých i malých písmen a znaků), nezjistitelné (př. hackerský program zkouší slova ze slovníku) a především unikátní – nikdy nepoužívejte stejné heslo pro různé služby (sociální sítě, e-mail a bankovní účet). Hesla s nikým nesdělujte a neukládejte je do prohlížeče. Pokud si je nezapamatujete, zapište si je, ale následně uložte na bezpečné místo. Pokud je to možné, zvolte k účtům dvoufaktorové ověřování.

Pozor na neznámé přílohy Nechvírejte e-maily ani přílohy od neznámých a podezřelých odesílatelů, neklikejte ani na žádné odkazy v těle těchto e-mailů. Vždy raději zkontrolujte e-mailovou adresu odesílatele a pravopis.

Nakupujte jen u prověřených on-line prodejců Přes internet nakupujte jen u prověřených a důvěryhodných prodejců – orientujte se podle ikony zamknutého visacího zámku u URL adres jejich webu, musí být bez jakéhokoli upozornění. To samé platí u přihlašování na jakýkoli web, bank zejména. U soukromých inzerentů a méně známých prodejců čtěte recenze.

Čtěte upozornění banky Nejen ta bankovní, ale také vašeho počítače. Pokud upozornění jen odklikнete, může vám např. uniknout zpráva z vaší banky o útocích hackerů. Věnujte jim pozornost a chraňte sebe i svůj účet.

Informujte banku Pokud máte byť jen podezření, že se s vaším účtem děje něco podivného či špatného, kontaktujte svou banku. Přes infolinku vám zákaznická podpora dokáže zkontrolovat váš účet a případně zablokovat příkazy.

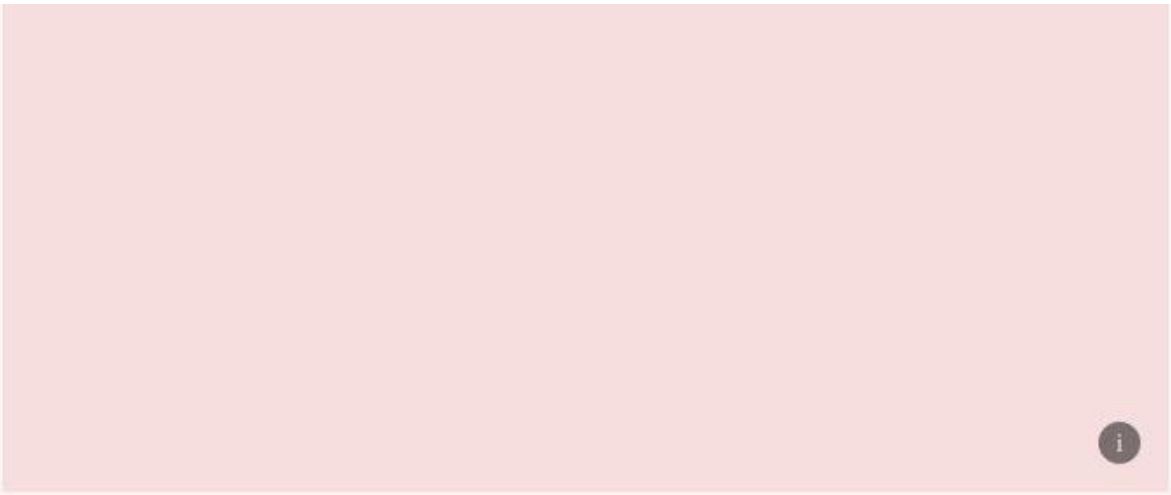
150. Nejlepší dárek může ušetřit statisíce. Ukažte rodině, jak fungují podvody

Online ● seznamzpravy.cz (Zprávy / Politika) ● 23. 12. 2022, 10:09

Vydavatel: **Seznam.cz, a.s. (cz-26168685)** ● Autor: **Pavel Kasík**

Dosah: 1 702 492 ● GRP: 18.92 ● OTS: 0.19 ● AVE: 79177.75 Kč ● Interakcí: 18

Odkaz: https://www.seznamzpravy.cz/clanek/tech-technologie-internet-nejlepsi-darek-muze-usetrit-statisice-ukazte-rodine-jak-funguji-podvody-221889



Nakupování na internetu je snadné… a stejně tak snadné je i skočit na lep internetovému podvodníkovi.

10:09

Víte, jak na internetu rozpoznat podvod? A vědí to i vaši rodiče, prarodiče a další příbuzní? Dejte jim pod stromeček možná nejcennější dárek. Naučte je, co na ně číhá. Vás to bude stát 20 minut času, jim můžete ušetřit statisíce.

Falešný bankéř, krádeže hesla, sňatkoví podvodníci i předražené přípravky na hubnutí.

Internet je plný hrozeb, které jsou na první pohled těžko rozpoznatelné. Možná se v těchto věcech dobře orientujete. Víte, že když vám někdo nabídne odvoz zboží zdarma přes objednaného kurýra, zasmějete se, protože víte, že je to známý podvod.

Ale vědí to i všichni členové vaší rodiny? Dost možná ne. Tak jim letos dejte pod stromeček něco výjimečného: svůj čas. Sedněte si s nimi, projděte nejčastější typy podvodů a hrozeb. Nastavte počítač a mobil tak, aby se jim lépe používal. A ubezpečte je, že se vás mohou kdykoli zeptat, pokud si nebudou vědět rady nebo jim nějaká nabídka přijde podezřelá. Dost možná jim tímto netradičním dárkem ušetříte desetitisíce nebo statisíce korun.

Sami si musíte rozhodnout, zda jste to zrovna vy, kdo by měl rodinným příslušníkům udělovat rady ohledně počítačové bezpečnosti. Ale nebojte, nebudete na to sami. Připravili jsme pro vás přehled materiálů, testů a videokurzů, které k tomu můžete použít.

Příklady vydají za tisíce slov

Pokud jste se rozhodli, že „bezpečnostním rychlokurzem“ někoho obdarujete, nezapomeňte přizpůsobit svůj výklad příjemci. Jinak budete hrozby na internetu vysvětlovat dětem, které s internetem vyrůstaly, a jinak lidem narozeným v 50. letech.

Ideální je se nejprve zeptat, jaké služby na internetu používají, zda mají nějaké otázky, s čím chtějí pomoci a co už o internetových podvodech vědí. Uvidíte, že vás svým rozhledem překvapí.

Nezapomeňte také ukázat nějaké konkrétní příklady. Je nesmírně poučné podívat se na reálné ukázky konverzace s podvodníkem, protože pak takový podvod snáze rozpoznáte, když se stanete jeho terčem.

Dobrým začátkem je nový projekt Kybertest.cz, který můžete s blízkými vyplnit za pár minut. Už jen během testu určitě přijdete na zajímavé oblasti, které pak můžete dále rozebrat.

Nástroj připravila Česká bankovní asociace. Seznam Zprávy jsou mezi mediálními partnery projektu.

Natrénovat rozpoznání phishingu můžete u testu od firmy Google. Je v češtině a obsahuje kromě příkladů i podrobné vysvětlení a simulaci reálného chování e-mailu.

Ukázky působí velmi realisticky. Můžete tak názorně ukázat, na co myší najet nebo kliknout, když si chcete ověřit, od koho mail je nebo kam vede přiložený odkaz.

Přímo na děti a mladistvé cílí výuková iniciativa Avastu: Buď Safe Online. Mladému publiku je přizpůsobena nejen jazykem, ale i specifickou probíranou problematikou, včetně třeba posílání nahých fotografií nebo kyberšikany.

Stránky kurzu Buď Safe Online.

Národní úřad pro kybernetickou a informační bezpečnost má zase pro děti kyberpohádky. Na míru starším obyvatelům pak NÚKIB ušil kurz Senior proti internetovým padouchům. Lekce je celkem krátká a probírá všechna hlavní témata.

Ukázka z kurzu NÚKIB.

Další kurzy má NÚKIB přímo na svých stránkách v sekci Nabízené kurzy, najdete zde materiály obecné i specificky zaměřené kupříkladu na pracovníky ve vzdělávání.

Pro zpestření výkladu můžete využít i audioukázky reálných podvodníků. Kolegové jich

nahráli celou řadu. Je to dobrá připomínka toho, jak důvěryhodně někdy může podvod po telefonu znít.

UKÁZKY INTERNETOVÝCH PODVODŮ:

Pozor na podvod. Takhle vás okradou přes telefon

29. 10. 8:49

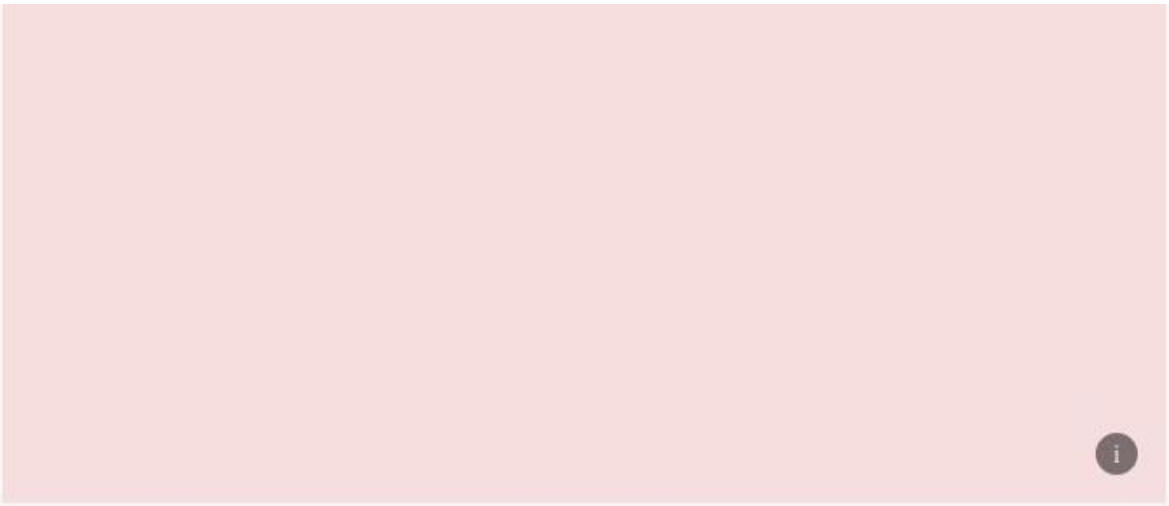
Nahrávka: pozor na podvodné telefonáty. Takhle vás okradou o tisíce

13. 9. 14:15

Pokud budete mít pocit, že je to do vánoční atmosféry celé moc pochmurné, připomeňte příbuzným, že se vám kdykoli mohou ozvat, když si nebudou jistí. Právě taková jednoduchá rada může mít největší dopad. Lidé se někdy bojí se zeptat. A útočníci toho využívají, někdy dokonce obětem výslovně zakazují, aby o telefonátu s někým mluvili.

„Bezpečností prověrka“ se hodí každému

Pokud si chcete připravit vlastní přednášku, můžete se inspirovat třeba stručným návodem Bezpečnost na internetu, který jsem před několika lety sestavil a postupně jej doplňuji.



Stručný návod, který může posloužit jako inspirace k „rychlokurzu pod stromeček“.

Stáhnout si můžete dvoustránkový dokument i kondenzovanou verzi, která se vejde na jednu A4.

Jak poznat podvodníky na internetu

Hlavní pozornost věnuji v manuálu popisu nejčastějších on-line podvodů:

- **Spam** aneb nevyžádaná pošta obvykle nabízí nákup nějakého zboží.
- **Phishing** vás přesměruje na falešný web, který se tváří jako oficiální, ve snaze vylákat z vás vaše údaje, číslo karty či heslo.
- **Falešný kurýr** slibuje vyzvednutí zboží.
- **Falešné články** se tváří jako publicistika, jde ale o „advertoriál“, smyšlený příběh, který vás má přesvědčit ke koupi přípravku.
- **Falešná faktura** nebo falešné upozornění ohledně nedostatku peněz mají za cíl vyděsit vás a vylákat z vás vaše údaje, nebo rovnou peníze.
- **Falešné seznámení**, kde podvodník předstírá, že je žena/muž toužící po vaší blízkosti, po několika dnech nebo měsících z vás lstí tahá peníze.
- **Vydírání údajnými citlivými záběry**, které útočník zveřejní, pokud mu nezaplatíte výkupné.
- **Nabídka zboží v bazaru**, kdy chce podvodník peníze předem nebo zadat kartu.
- **Nabídka rychlého výdělku** bez práce: kryptoměny, binární opce, gambling, vícestupňový marketing, investice...
- **Falešná technická podpora** bude chtít na váš počítač nainstalovat software pro vzdálený přístup, a tak jej ovládnout.

- **Falešný policista nebo bankéř** bude tvrdit, že nesmíte nikomu o hovoru říci.

Důležitější než jednotlivé podvody jsou obecné principy: časová tíseň, vzbuzování strachu, ohánění se autoritou, snaha donutit oběť k rychlé akci…

Výhodou je, že si návod můžete stáhnout ve formátu DOCX a upravit na míru potřebám vaší domácnosti. Můžete si také stáhnout můj návrh, co všechno byste měli v domácnosti nastavit tak, aby bylo zabezpečení na dobré úrovni. Taková *bezpečnostní prověrka* může ostatně jednou za čas prospět každému. Nejen o Vánocích.

SDÍLEJTE ČLÁNEK