



ČESKÁ CZECH
BANKOVNÍ BANKING
ASOCIACE ASSOCIATION



Než začneme...

Vyzkoušejte si **KYBERTEST!**
www.kybertest.cz





Tisková konference 13. července

KYBER | TEST BEZPEČNOST

KYBERKAMPAŇ:
CÍLEM HACKERA MŮŽETE
BÝT I VY!





Petr Barák

předseda Komise ČBA
pro bankovní a finanční bezpečnost



Zuzana Pidrmanová

vedoucí oddělení prevence
Policejního prezidia ČR



Ondřej Kapr

Úřad služby kriminální policie a
vyšetřování



Robert Šuman

vedoucí pražského výzkumného
oddělení společnosti ESET

ÚVOD

- Digitalizace bankovníctví -> přesun bankovníctví z kamenných poboček bank do mobilních telefonů a počítačů.
- Rozvoj bankovních služeb není spojen s rozvojem klientských znalostí v oblasti kybernetické bezpečnosti:
 - Index kyberbezpečnosti ČBA (měřen v rámci průzkumu veř. mínění): úspěšnost dlouhodobě na 60 %
 - V 2020 ověření výsledků průzkumu v praxi pomocí praktického testu: úspěšnost 43 %
- Banky masivně investují do svého technického zabezpečení, nastavují nové bezpečnostní mechanismy (dvoufaktorové ověřování, biometrie...).

NEJZRANITELNĚJŠÍ ČLÁNEK V ŘETĚZCI = KLIENT

- Banky se snaží své klienty chránit a maximálně jim pomoci, ale pokud klient hrubě poruší bezpečnostní pravidla, nemůže očekávat, že mu banka škodu uhradí -> je odkázán na OČTŘ, aby škodu vymáhal na pachateli trestného činu.





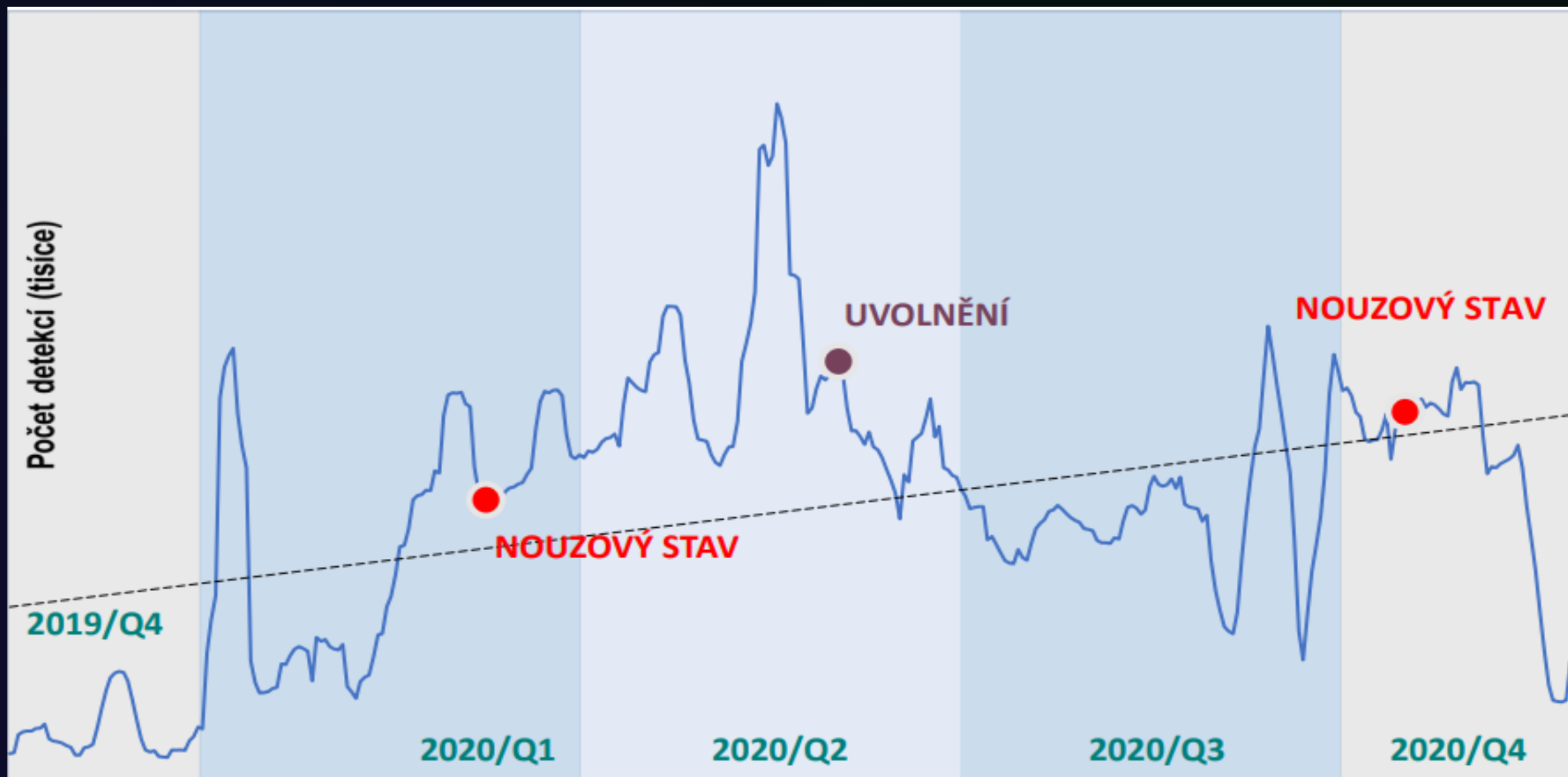
PHISHING & VISHING

PHISHING

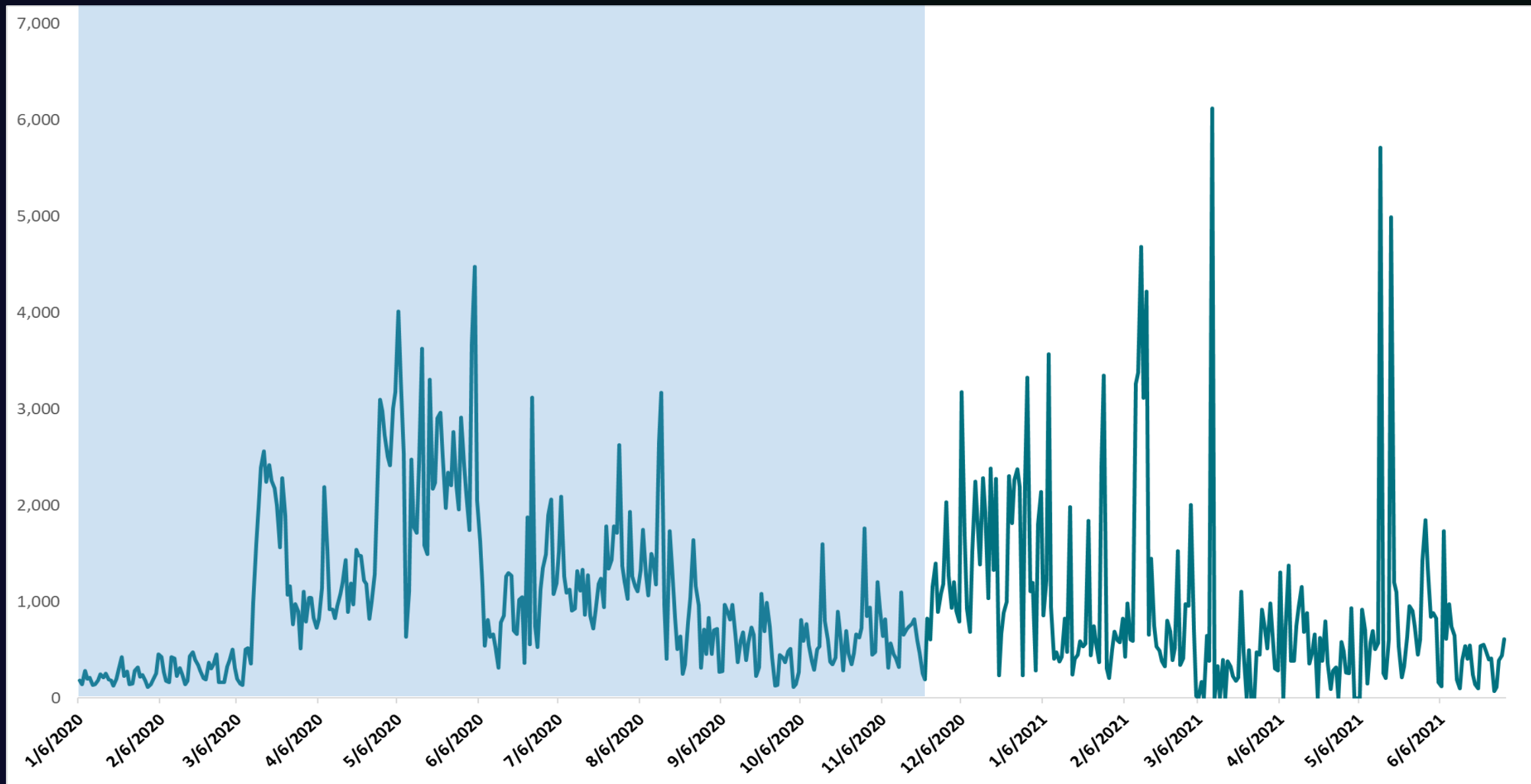
- Podvodná technika k získání citlivých údajů a ve finále jejich monetizace (údaje z platební karty, přihlašovací údaje do internetového bankovníctví apod.).
- Metoda „kobercového náletu“ aneb principem je plošné zasílání e-mailových či SMS zpráv na adresy či jiné údaje, které získali například z profilů obětí na sociálních sítích, datových úniků firem a institucí
- Dnes často velice zdařilé a důvěrně vypadající e-maily bez překlepů a gramatických chyb, tváříci se jako oficiální zprávy banky, pošty, obchodního řetězce či dalších institucí
- Příklad v případě „falešné zprávy banky“:
 - e-mail/SMS o uzamčení účtu s odkazem na odemčení, který směřuje na falešné stránky,
 - e-mail/SMS o zablokování karty s odkazem na odblokování či výzvou k zaslání údajů.
- Součástí zpráv může být: časový nátlak, někdy špatná gramatika, podezřelé odkazy, či tlačítka vedoucí na falešné stránky, nadměrně velké přílohy obsahující malware...



PHISHING v datech (události)



PHISHING v datech (unikátní adresy)



VISHING



- Relativně nová podvodná metoda založená na plošných a cílených útocích skrze telefonní hovor – „voice phishing“.
- Obecně je cílem pachatelů zjištění informací a manipulace oběti do nějakého jednání.
- Technika založená na vyvolání strachu a naléhavosti ihned konat, nebo snadného finančního zisku.
- Evidujeme převážně 3 druhy vishingu dle modu operandi:
 - Donucení ke sjednání vzdáleného přístupu do zařízení – Falešná technická podpora a Podvodné investice.
 - Vylákání informací ohledně platebních prostředků
 - Manipulace do nějaké činnosti – Falešný bankéř



VISHING



- **Falešný bankéř.** Jedná se o cílený útok, kdy se pachatel vydává za pracovníka Vaší banky a je na Vás aby jste zachránili své finanční prostředky převodem na jiný účet. V poslední době po Vás pachatel žádá nákup bitcoinů za hotové peníze.
- Pozor na zdání falešného bezpečí „na účtu nemám žádné peníze“, „mně se to stát nemůže“.
- Nebezpečnost spočívá v kombinaci informovanosti pachatele o svých obětech, v manipulativním jednání a o použití **spoofingu**.
- Spoofing se může objevovat u i tzv. Smishingu.
 - Tiger kidnapping ve Velké Británii.
 - -> jednání ČBA s operátory a Českým telekomunikačním úřadem.



ÚTOKY NA KLIENTY ČESKÝCH BANK

- **Rok 2020**
 - Phishing: desetitisíce útoků, několikrát více než v roce 2019.
 - Vishing: nízké stovky, začátek tohoto typu podvodu.
- **Rok 2021 (leden až květen)**
 - Phishing: loňský rok je nyní co do počtu prakticky dorovnán.
 - Vishing: prudký nárůst, 6x více útoků než za celý loňský rok.
- Díky obezřetnosti klientů (tj. klient útok včas nahlásí...) a aktivitě bank (tj. zablokování podezřelé transakce či chargeback...) se v tuto chvíli (2021) daří **zastavit naprostou většinu útoků = 86 %**
 - (platí pro vishingové i phishingové útoky).



5 RAD PRO BEZPEČNÝ POHYB V KYBERPROSTORU

1. Nikdy nikomu nesdělujte své přihlašovací údaje do internetového bankovníctví ani čísla ze své platební karty. Banky se na ně opravdu NIKDY neptají, a to ani telefonicky, ani e-mailem, ani SMS či jinými zprávami. Zároveň nikdy neposílají odkazy na weby, kde jsou údaje vyžadovány! Ani Policie ČR nikdy občany nevyzývá k provádění bankovních transakcí nebo poskytování osobních údajů dalším osobám!
2. 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 kroky pro jejich záchranu. Kdyby byly vaše peníze skutečně v ohrožení, banka by již zareagovala dávno a bez vaší pomoci.
3. Nezasílejte ani v aplikaci nepotvrzujte platby, které by vám někdo chtěl diktovat po telefonu. Stejně tak nedávejte nikomu vzdálený přístup do vašeho počítače.
4. Mějte aktualizovaný software a antivirus v PC i telefonu. Aplikace stahujte jen z oficiálních zdrojů a nedávejte jim více oprávnění, než potřebují.
5. Buďte vždy v pozoru, nenechte se zviklat ani nalákat. V případě pochybností vždy kontaktujte svou banku či volejte Policii (158).





DALŠÍ ČASTÉ METODY ÚTOČNÍKŮ

FALEŠNÉ STRÁNKY E-BANKOVNICTVÍ

- Útočník chce získat přihlašovací údaje oběti s pomocí falešné webové stránky banky.
 - Ta může vypadat úplně stejně jako skutečný web banky, včetně loga a barev.
 - Někdy ji odhalit lze, např. URL adresa webu se odchyluje od oficiálního názvu či zkratky banky, na stránce jsou překlepy, v řádku s adresou nebude visací zámek označující bezpečnostní certifikát webu, nýbrž upozornění apod.
- Pomocí dalších podvodných technik pak získá potvrzovací kód, autorizační SMS či přístup k mobilnímu klíči.
- Známá útočná metoda – již není tolik využívána jako dříve, neboť je pracná a současně speciální SW je umí včas odhalit.

JAK SE CHRÁNIT

- Jako před phishingem a vishingem, tj.
- -> být pozorný
- -> neklikat na podezřelé odkazy a nechodit na nezabezpečené weby,
- -> nainstalovat na zařízení bezpečnostní software,
- -> mobilní aplikace nakupovat nejlépe jen na Google Play či App Store, číst jejich recenze a nedávat jim více oprávnění, než potřebují.



ZÍSKÁNÍ NADVLÁDY NAD PLATEBNÍ KARTOU V MOBILU

- Útočník pomocí nějaké podvodné metody získá údaje o platební kartě oběti a tzv. ji digitalizuje
 - = nahraje ji do svého telefonu, resp. do Google Pay či Apple Pay, a registraci potvrdí aktivačním kódem (zasílaným do internetového bankovníctví či SMS).
- Následně již může platit svým telefonem a odčerpávat oběti peníze z účtu, dokud si toho nevšimne.

JAK SE CHRÁNIT

- Kontrolovat pravidelně stav svého účtu a odcházející platby.
- Jako před phishingem a vishingem, tj.
 - -> být pozorný
 - -> neklikat na podezřelé odkazy a nechodit na nezabezpečené weby,
 - -> nainstalovat na telefon bezpečnostní software,
 - -> mobilní aplikace nakupovat nejlépe jen na Google Play či App Store, číst jejich recenze a nedávat jim více oprávnění, než potřebují,



PODVODNÉ MOBILNÍ APLIKACE

- 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 při instalaci aplikaci udělíte vysoká oprávnění – například aplikaci pro nahrávání hovorů i přístup k fotoaparátu či SMS – dokáže odcizit vaše přihlašovací údaje do bankovníctví, obejít dvoufázové ověření či získat potvrzovací SMS zprávy.

JAK SE CHRÁNIT

- -> Nainstalovat na telefon bezpečnostní software.
- -> Aplikace nakupujte nejlépe jen na Google Play či App Store, čtěte jejich recenze a nedávejte jim více oprávnění, než potřebují.



VYDÍRÁNÍ (DOXING & RANSOMWARE)

- Po krádež dat od firem a institucí, které je měly špatně zabezpečeny, následuje nabídka hackerů je odkoupit zpět
- Použití zejména dvou metod:
 - **ransomware** = vyděračský software, který blokuje počítačový systém, dokud oběť nezaplatí výkupné.
 - **doxing**
 - vznikl jako reakce na menší účinnost kampaní využívajících ransomware (pokud uživatel či firma ale správně zálohuje, ransomware je neohroží a útočník přijde o výkupné)
 - Při doxingu útočník oběti vyhrožuje zveřejněním získaných dat, což pro firmu představuje reputační riziko, ale i riziko ztráty dat z výzkumu, interních informací, obchodních tajemství apod.

JAK SE CHRÁNIT

- -> Uchovávat ve svých zařízeních a systémech pouze to, co je skutečně nezbytné a to zálohovat.
- -> Chránit systémy účinným a aktuálním bezpečnostním software, využít služeb specializovaných firem



FALEŠNÉ & KRAĐENÉ PROFILY NA SOCIÁLNÍCH SÍTÍCH

- Útočníci typicky vytvoří falešný či zcizí profil osoby, kterou oběť zná a pak z tohoto profilu po oběti žádají formou zprávy provedení nějaké akce
 - vyplnění formuláře, zaslání finanční částky na pomoc
 - pod záminkou výhry v soutěži, upozornění před nebezpečím apod. posílají odkazy směřující na falešné stránky sloužící k získání údajů z platební karty, přihlašovacích údajů do e-bankovníctví či jiných důvěrných údajů oběti.

JAK SE CHRÁNIT

- Výzvu si s danou osobou raději telefonicky ověřit
- Jako před phishingem a vishingem, tj.
- -> být pozorný
- -> neklikat na podezřelé odkazy a nechodit na nezabezpečené weby,
- -> nainstalovat na zařízení bezpečnostní software,
- -> mobilní aplikace nakupovat nejlépe jen na Google Play či App Store, číst jejich recenze a nedávat jim více oprávnění, než potřebují.





KYBERKAMPAŇ

KYBERKAMPAŇ

- Edukační preventivní kampaň zaměřená na prevenci proti současným masivním vlnám phishingových a vishingových útoků.
- Realizátor: Česká bankovní asociace a Policie ČR (vč. krajských koordinátorů - preventistů) ve spolupráci se společností ESET.
- Zapojení: členské banky ČBA, společnost Zásilkovna, Hospodářská komora ČR, ICT Unie a další.
- Hlavní sdělení:
 - Cílem hackera můžete být i vy!
 - I jedna chyba vás může stát všechny vaše úspory!
- Kanály: online sociální sítě, mailing + outdoor.
- Obsah kampaně:
 - edukativní videa,
 - letáčky, plakáty, prostírání v restauracích,
 - středobod kampaně = webová aplikace kybertest.cz.



I JEDNA CHYBA VÁS MŮŽE STÁT VŠECHNY

5 RAD PRO BEZPEČÍ VAŠICH PENĚZ

1. Nikdy nikomu nesdělujte své přihlašovací údaje do internetového bankovníctví ani čísla ze své platební karty. Banky se na ně neptají, ani zprávami či e-mailem neposílají odkazy na weby, kde jsou vyžadovány!
2. 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 kroky pro jejich záchranu. Kdyby byly vaše peníze v ohrožení, banka zareagovala dříve už bez vás.
3. Pány svého účtu jste jen vy. Nezádávejte 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.
4. Mějte aktualizovaný software a antivirus. A to i na telefonu!
5. V případě pochybností vždy kontaktujte svou banku či volejte 158. Myslete na to, že útočník dokáže napodobit jakékoliv telefonní číslo (tzv. spoofing) či e-mail, vč. těch vaší banky.

POZOR! Chce po vás někdo jménem vaší banky přístupové údaje do internetového bankovníctví? NEBO abyste provedli platbu platební kartou? NEBO abyste provedli platbu důvodu hrozícího útoku na váš účet?

NEREAGUJTE, JDE O PODVODNÍK! KONTAKTUJTE VAŠI BANKU ČI VOLEJTE 158.

Přežijete v online světě? Vyzkoušejte si **KYBERTEST!** www.kybertest.cz



Ukázka podvodného telefonátu

Dobrý den, jsem Jan Novák z oddělení bezpečnosti vaší banky. Omlouvám se, že vás vyrušuji takto pozdě večer. Dovolím jsem se paní Marii Krasné s běžným účtem č. 123456789/0 u Rodinné banky?

Ano, to jsem já. Co se děje?

Zaznamenali jsme několik podezřelých přihlášení k vašemu účtu, jeden dokonce z Gruzie.

Prosím? To není možné! Jsem v Česku...

Máme podezření, že váš účet byl napaden. Pokud máme zcizení peněz zamezit, potřebujeme neodkladně vaši rychlou spolupráci. Přihlaste se do vaší aplikace a potvrďte kód, který jste obdržela.

#PHISHING podvodné zprávy, e-maily

#KYBERTEST

#VISHING volání falešných bankéřů

Vážený zákazníku, děkujeme, že využíváte služby Rodinné banky. Jasně.

KYBERTEST

- Speciálně připravený online interaktivní kvíz, kterým respondenty provází česká **fiktivní banka „Rodinná banka“**.
- 10 obrázků (otázek) ukrývající 0 až 4 podezřelých prvků, které mohou naznačovat útok hackera.
- Otázky představují situace, do kterých se uživatelé internetu běžně dostávají – přihlášení se do internetového bankovníctví, stažení bankovní aplikace v internetovém obchodě, e-mailová komunikace.
- Cílem uživatelů je v časovém limitu prvky odhalit.
- Součástí i edukační obsah – stránky s desaterem a nejčastějšími hackerskými útoky.
- Více na <https://kybertest.cz/>





DOTAZY & DISKUZE

DĚKUJEME ZA POZORNOST!

