**Kybertest: Falešné stránky internetového bankovnictví Češi s jistotou nepoznají, podvodné SMS u nich naopak nemají šanci**

Interaktivní kvíz ČBA, společnosti ESET a Policie ČR odhalil slabé stránky Čechů. Zúčastnilo se ho bezmála 100 tisíc lidí.

**Praha, 16. září 2021 – Nejsnáze rozeznají Češi „férovou“ aplikaci a podvodné SMSky, naopak nejvíce problémů mají s falešnými přihlašovacími stránkami a podvodnými e-maily. Vyplývá to z dosavadních výsledků Kybertestu, který je součástí společné edukační Kyperkampaně ČBA, společnosti ESET a Policie ČR. Interaktivní kvíz si doposud vyzkoušelo bezmála 100 tisíc Čechů s průměrnou úspěšností 52 %. Úspěšnější v odhalení podvodů jsou přitom spíše muži a uživatelé ve věku do 34 let. S vyšším věkem jsou Češi zranitelnější, potvrzují průběžná zjištění.**

V rámci testu si každý uživatel může ověřit, zda v praktických příkladech rozezná nejčastější triky útočníků jako jsou podvržené odkazy, webové stránky nebo odkazy. Kybertest spustily v polovině července společně Česká bankovní asociace (ČBA), Policie České republiky a společnost ESET, jakožto stěžejní prvek osvětové Kyberkampaně, která měla a má varovat před narůstajícími počty vishingových a phishingových útoků. Podle dat z roku 2020 totiž většina uživatelů své znalosti rizik přeceňuje. A útočníci jsou si toho velmi dobře vědomi.

*„Útoky hackerů jsou stále sofistikovanější. Již dávno to není o e-mailech plných chyb, kde jsme na první pohled schopni rozpoznat, že něco není v pořádku. Útoky jsou dnes předem promyšlené a jejich cílem je v nás s pomocí sociálního inženýrství vyvolat strach o naše peníze uložené na účtu v bance. Zároveň v nás útočníci chtějí vyvolat pocit, že oni jsou ti, kteří nám chtějí pomoci, a právě jim bychom měli sdělit naše citlivé údaje,“* říká Petr Barák, předseda Komise ČBA pro bankovní a finanční bezpečnost, a doplňuje: *„Scénářů je celá řada, podvodníci se již nevydávají pouze za policisty či bankéře, ale např. i za finanční správu či ČNB. V poslední době se začínají ve stále větší míře objevovat i různé podvodné investiční nabídky, kdy se pachatelé snaží klientům bank zprostředkovat velice výhodné uložení jejich úspor do různých komodit, jako jsou cenné kovy nebo kryptoměny s tím, že se o vše za ně postarají a „je pouze třeba“ jim umožnit přímý přístup do jejich internetového bankovnictví. Pokud jim toto klient umožní, dochází nejen k odcizení všech uložených úspor na účtu ale mnohdy i jménem klienta k podání nové žádosti o úvěr a následně i k odcizení těchto prostředků. Nejsou výjimkou ani případy, kdy je pachateli účet klienta, který oni sami ovládli, využíván k přesouvání finančních prostředků, odcizených z dalších klientských účtů, tedy fakticky k legalizaci výnosů z trestné činnosti.“*

**Testují se běžné scénáře útočníků**

Kybertestem uživatele provází fiktivní Rodinná banka a následně řada situací, do kterých se jako uživatel internetu a klient banky běžně dostává např. e-mailová komunikace, přihlašovací stránky či aplikace ke stažení. Úkolem účastníků je pak v rámci jednotlivých ilustračních obrázků poznat, zda obsahují tzv. podezřelé prvky.

„*Potenciálně rizikovým neboli podezřelým rozumíme cokoliv od překlepu ve větě, přes podezřelou adresu odesílatele až po propadlý certifikát webové stránky. Nic z toho zpravidla není jednoznačným indikátorem, že se jedná o podvodnou aktivitu útočníka, ale je to pro nás jako pro uživatele znamení, že by zde mohlo být něco v nepořádku. Pokud je podobných prvků na webové stránce či e-mailu více, riziko toho, že jsme terčem podvodu, se výrazně zvyšuje,”* vysvětluje Robert Šuman, vedoucí pražského výzkumného oddělení společnosti ESET.

V případě přihlašovací stránky do internetového bankovnictví lidé nejčastěji přehlédli drobná zaškobrtnutí útočníků, jako například neaktuální SSL certifikát nebo překlepy v textu stránky. Naopak bez větších problémů si lidé všimnou podvržené URL adresy. Velmi dobře dokázali uživatelé také identifikovat podvodné SMS nebo falešnou výzvu k obnovení přístupu do internetového bankovnictví.

U phishingu, který vyzýval k obnovení údajů uživatele respondenti správně identifikovali falešnou adresu odesílatele a podvržený odkaz. Vše uvedené jsou běžné praktiky útočníků. Odborníci radí vždy prověřovat, od koho přesně zprávy přicházejí, ještě před tím, než uživatel stáhne přílohu či otevře přiložený odkaz. „*Obecně nejméně chyb zachytili uživatelé na falešné přihlašovací stránce a v případě podvodné aplikace. V rámci testu se objevují také e-maily vyhrožující exekucí. Jde o trik, který používají útočníci k šíření malware už léta. Pro mě překvapivě u této otázky respondenti dosahovali úspešnosti jen 45 %. Zřejmě nejsnazší byla otázka na legitimní aplikaci banky, kde úspěšnost dosahovala 79 %,*“ říká Robert Šuman.

Jen třetina uživatelů také správně určila všechny podezřelé prvky při simulaci stažení aplikace. Zejména uživatelé přehlédli chybné zařazení aplikace do nerelevantní kategorie a také méně pravděpodobné jméno vývojáře, v kontextu té konkrétní aplikace. V otázce, kde si uživatel stahoval legitimní aplikaci lidé odpovídali spíše správně. Svědčí to o tom, že jako uživatelé aplikace příliš neprověřujeme. Samotné jméno vývojáře, nízký počet stažení nebo chybná kategorie aplikace nemusí nutně znamenat podvodnou aplikaci. Vždy je třeba vše vnímat v celkovém kontextu. Pokud ale narazíme na více než jeden podezřelý prvek, riziko, že se jedná o rizikovou aplikaci, se výrazně zvyšuje. V takovém případě bychom měli zvážit, zda ji skutečně chceme stáhnout.

**Muži a mladí uživatelé si vedou lépe**

Podle dosavadních dat si o něco lépe vedou muži než ženy. Přesněji například dokázali identifikovat podvodný e-mail vyhrožující exekucí (11% rozdíl ve správnosti odpovědí), falešnou aplikaci a podvodný e-mail se škodlivým odkazem (7% rozdíl). Naopak není zřejmý rozdíl mezi odpověďmi lidí z velkých měst a vesnic.

Nejhůře v testu naopak dopadli senioři, kybernetická bezpečnost je spíše doménou mladších uživatelů mezi 18. a 34. rokem. Nejvýraznější rozdíly byly u otázek s přihlášením do internetového bankovnictví a při identifikaci legitimní mobilní bankovnictví aplikace.

**Uživatele ochrání vlastní obezřetnost**

ESET zablokoval jen v první polovině letošního roku průměrně přes deset tisíc phishingových útoků denně, oproti roku 2020 se nicméně jedná o zhruba třetinový pokles. Rok 2020 byl v tomto ohledu extrémní, útočníci totiž významně zneužívali nejistotu lidí v souvislosti s koronavirem. Další podvody odfiltrují spamové filtry v e-mailových schránkách uživatelů. Phishing se objevuje ve vlnách, útočníci reagují na významné společenské události a svátky. Útoků tedy přibývá například se začátkem školního roku, v období adventu nebo v Česku také experti zachytávali intenzivní kampaně v reakci na vyhlašování proti pandemických opatření. Obecně platí, že útočníci se snaží využít období, kdy sedíme u počítačů, ale jsme méně pozorní.

I podle údajů policie se značná část zločinců přesouvá do kybernetického prostoru. Je zcela klíčové, aby uživatelé prověřovali různé požadavky a aktivně si tak chránili data i úspory.

„*Policie České republiky skutečně zaznamenává úbytek „klasické kriminality“, je však patrný přesun nápadu protiprávního jednání do kybernetického prostoru. Problém je v tom, že kriminalita páchaná v kyberprostoru je velice dynamická a útočníci užívají jak ověřené techniky, jako je například phishing nebo různé podvody, které jsou spojeny s nákupem zboží přes internet, tak i zcela nové techniky nebo modifikované scénáře, které dovedou nepřipraveného uživatele internetu zcela zaskočit. Valná většina útoků je ale stále založena na oklamání uživatele, který je nejzranitelnějším článkem kybernetické bezpečnosti. Proto je důležité se nad svým chováním na internetu zamýšlet a nekonat nic zbrkle a bezmyšlenkovitě. Útočníci nejčastěji používají techniky sociálního inženýrství, které jsou založeny na jednoduchých, ale bohužel stále funkčních principech. Jedná se o vyvolání pocitu strachu, zvědavosti a ziskuchtivosti. Dokonce i opravdu sofistikované kybernetické útoky využívají vektor útoku právě skrze lidský faktor,*“ popisuje plk. Kateřina Zemanová, vedoucí odboru hospodářské kriminality Úřadu služby kriminální policie a vyšetřování.

Experti proto apelují na uživatele, aby všem neobvyklým e-mailům, SMS a zprávám v chatovacích aplikacích věnovali dostatečnou pozornost a důkladně si nejprve ověřovali, zda je daný požadavek legitimní. Totéž platí i při vishingu, neboli podvodném telefonátu. Útočníci v rámci podvodných telefonátů totiž začínají využívat tzv. spoofing neboli vydávání se za někoho jiného. *„Pokud má klient číslo své banky v telefonu uloženo, mohou ho útočníci pěkně zmást. Princip podvodných telefonátů je přitom téměř vždy stejný. Útočník chce klienta vystrašit a zároveň vzbudit důvěru, že on je tím, kdo mu pomůže ochránit peníze na účtu,*“ upozorňuje Petr Barák z ČBA.

„*Vždy bych doporučil v první řadě ověřit, zda je volající nebo odesílatel skutečně osobou, za kterou se vydává a se kterou můžete otevřeně jednat. Pokud nedochází k osobnímu jednání, můžete podobně ověřit i webové stránky. V tomto velice pomáhá bezpečnostní program, který řadu podvodů odfiltruje za vás,“* radí Robert Šuman.

„*Je důležité si pamatovat, že banky ani Policie nikdy nevyžadují citlivé informace jako jsou hesla, přihlašovací údaje do internetového bankovnictví, čísla platebních karet či jejich CVV kódy ani jakýkoliv vzdálený přístup do klientova počítače a jeho internetového bankovnictví. Pokud od vás kdokoli takové údaje nebo přístupy požaduje, nesdělujte a nepovolujte mu je, komunikaci ukončete a kontaktujte svou banku,*“ připomíná Petr Barák z ČBA.

**Osvěta je ale stále důležitá „Cílem hackera můžete být i vy!“**

V souvislosti s nárůstem vishingových i phishingových útoků a také faktem, že ze strany veřejnosti jsou tyto útoky stále značně podceňovány, je edukace v současné době o to důležitější*.* I proto bude Kyberkampaň s hlavním sdělením „Cílem hackera můžete být i vy!“ pokračovat, a to zejména formou edukativních videí a bannerů na sociálních sítích či plakátů a letáčků.

Nově bude osvěta o problematice přibližována veřejnosti ale i prostřednictvím televizních obrazovek v městské hromadné dopravě (TV BUS) ve vybraných lokalitách ČR. Zároveň bude Kybertest začleněn do projektu Bankéři do škol, který bude letos probíhat během října a do kterého se mohou zapojit žáci 8. a 9. tříd základních škol nebo studenti 1. a 2. ročníků středních škol napříč republikou.

Kromě stávajících institucí, které se do projektu zapojily a kterými jsou členské banky ČBA, společnost Zásilkovna, Hospodářská komora ČR, ČNB či Asociace hotelů a restaurací, se nově zapojí i Národní úřad pro kybernetickou a informační bezpečnost, který projekt zařadí do svého rozcestníku pro inspiraci výuky kybernetické bezpečnosti, či Ministerstvo vnitra, prostřednictvím něhož budou letáky k uvedené problematice distribuovány na každý obecní úřad v České republice.

plk. Zuzana Pidrmanová

vedoucí oddělení prevence

Policejní prezidium ČR

zuzana.pidrmanova@pcr.cz

tel: + 420 974 834 375

**O Policii ČR**

Policie České republiky je jednotný ozbrojený bezpečnostní sbor zřízený zákonem České národní rady ze dne 21. června 1991. Slouží veřejnosti. Jejím úkolem je chránit bezpečnost osob a majetku, chránit veřejný pořádek a předcházet trestné činnosti. Plní rovněž úkoly podle trestního řádu a další úkoly na úseku vnitřního pořádku a bezpečnosti svěřené jí zákony, předpisy Evropských společenství a mezinárodními smlouvami, které jsou součástí právního řádu České republiky. Předcházení kriminalitě realizací preventivních aktivit je důležitou součástí činnosti Policie České republiky.

Ondřej Šafář

manažer PR a komunikace ESET

ondrej.safar@eset.cz

tel: + 420 776 234 218

**O společnosti ESET**

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio produktů ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

Andrea Trudičová

PR a komunikace ČBA

andrea.trudicova@cbaonline.cz

tel: + 420 734 638 103

**Další informace obdržíte na adrese:**

**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 37 členů. Rolí asociace je především zastupovat a prosazovat společné zájmy členů, prezentovat roli a zájmy bankovnictví vůči veřejnosti, podílet se na standardizaci postupů vbankovnictví 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 aEMMI. Více informací na www.cbaonline.cz