Falešné výhry, zablokované účty i pokuty – součástí kyberpodvodů v Česku byly ve druhém čtvrtletí online reklamy

12.8.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Kyberpodvody v Česku se při srovnání s prvním čtvrtletím letošního roku během dubna až června proměnily. Útočníci chtěli získat naše osobní či platební údaje prostřednictvím škodlivých webových stránek. Manipulovali nás falešnými oznámeními o výhře v online kasinu, zneužívali naše obavy kvůli možnému zablokování účtu nebo nezaplaceným dopravním pokutám. Komunikaci šířili prostřednictvím reklamních kampaní a vyskakovacích oken.

- Nejčastěji byly tyto případy monitorovány jako profesionálně skrytá phishingová komunikace, kterou experti z ESETu označují jako Agent.HVI. Hned v závěsu za tímto typem hrozby se v Česku nadále objevují detekce kyberpodvodů označené jako Phishing.Gen.
- V červnu pak po zhruba ročním klesání počtu detekcí opět mírně narostly případy investičního podvodu Nomani.

Praha, 12. srpna 2026 – Kyberpodvodníci se ve druhém letošním čtvrtletí nejčastěji zaměřovali na naše osobní data a přihlašovací údaje. Jako prostředek k dosažení tohoto cíle zvolili falešnou komunikaci prostřednictvím různých vyskakovacích oken nebo online reklamy, která vedla na škodlivé webové stránky s formuláři. Vyplývá to z analýzy phishingových útoků na Českou republiku od společnosti ESET za období od dubna do června 2026. Manipulativní komunikace opět pracovala s našimi emocemi – podvodníci tentokrát využívali falešná oznámení o výhře v online kasinu či zablokovaných účtech. Objevovala se také falešná výzva k zaplacení dopravních pokut. V červnu pak bezpečnostní experti opět zachytili mírný nárůst počtu investičních podvodů Nomani.

Zatímco ještě na začátku letošního roku bylo jedním z nejvíce frekventovaných útoků v našem regionu falešné hlasování v soutěžích prostřednictvím komunikační platformy WhatsApp, ve druhém čtvrtletí 2026 se počet těchto případů výrazně snížil. Znatelně se propadly také detekce podvodné komunikace, kterou bezpečnostní experti z ESETu sledují jako Phishing.Gen – z podílu dvou třetin všech zachycených útoků v prvním čtvrtletí na méně než jednu třetinu ve druhém čtvrtletí. Útočníci cílí podvody Phishing.Gen globálně a komunikaci vydávají za zprávy od celé řady firem, značek a institucí.

„Nejčastější internetové podvody v Česku jsme v období od dubna do června sledovali pod označením Agent.HVI. Jedná se o různorodé případy a scénáře podvodné komunikace. Jejich společným znakem je nicméně způsob šíření – pomocí reklamních kampaní a vyskakovacích oken, které vedou na škodlivé webové stránky s formuláři. Cílem je vyhnout se odhalení bezpečnostním softwarem. Jak můžeme vidět, útočníci věnují náležitou péči nejen ransomwaru či infostealerům, ale i podvodné komunikaci. Je to jen další důkaz, že phishing se jako kyberhrozba stále více profesionalizuje," říká Ondřej Novotný, kyberbezpečnostní analytik z pražské výzkumné pobočky společnosti ESET.

Cílem jsou jakákoli osobní data, cesta k nim vede přes náš strach

Ačkoli se nejčastější phishingové útoky tentokrát nezaměřovaly pouze na Českou republiku a řada falešných zpráv a výzev mohla být v angličtině, bezpečnostní experti je rozhodně nepovažují za méně nebezpečné.

„Podvodná komunikace začala ve druhém čtvrtletí nejčastěji jako vyskakovací okno nebo online reklama na sociálních sítích či v reklamním systému. Uživatelé a uživatelky uviděli nějakou senzační zprávu, že například vyhráli iPhone nebo mají zatočit kolem štěstí. V těchto případech vždy něco vyhráli. Pro účely předání výhry pak útočníci požadovali zadat kontaktní údaje či dokonce údaje o platební kartě. Následně se mohlo stát několik věcí – oběti mohly být registrovány k existujícím placeným službám, útočníci údaje mohli předat falešným call centrům, pokusit se zneužít platební karty nebo využít získané údaje k dalším phishingovým útokům. Obdobně se mohli uživatelé a uživatelky setkat s falešnou výstrahou, že mohou přijít o svůj účet na Facebooku. Úspěšnost této podvodné komunikace stojí na jednoduchém předpokladu – komunikace nás zaujme, vyvolá v nás pocit štěstí z výhry nebo strach ze ztráty účtu či peněz a my snáze uděláme, co se po nás chce. Všechno je to velmi rychlé a útočníkům se daří působit stále přirozeněji a důvěryhodněji," vysvětluje Novotný.

Práce se strachem pak byla ve sledovaném období typická i u jednoho scénáře v rámci detekce Phishing.Gen. Zde podvodníci rozesílali falešné SMS o údajné dopravní pokutě.

„Zpráva o falešné dopravní pokutě obsahovala odkaz na phishingový web. Útočníci zde pracovali s hrozbou neuhrazení pokuty a z toho plynoucích důsledků. Falešné stránky pak obsahovaly také informaci o tom, že lze získat slevu. Hlavním cílem útočníků bylo opět vylákat osobní data nebo údaje k platební kartě přes falešný webový formulář. Na základě naší analýzy vidíme, že útoky byly připraveny pomocí nástrojů a infrastruktury čínského původu," dodává Novotný.

Červnový nárůst případů investičního podvodu Nomani

Investiční podvody, které ESET sleduje pod označením Nomani, byly v České republice nejčastější ve druhém čtvrtletí loňského roku. Po postupném klesání počtu detekcí v následujících měsících začal jejich počet letos v červnu zase narůstat.

„Podvody Nomani jsou typické tím, že jsou jejich součástí upravené fotografie nějakých známých osobností, například celebrit a politiků. Velmi známým příkladem jsou falešné bulvární články s Andrejem Babišem. Není neobvyklé, že podvodníci k jejich přípravě používají nástroje umělé inteligence a tvoří tzv. deepfake obsah," říká Novotný.

Podvod Nomani má zpravidla několik dějství. Začíná jako nějaká chytlavá reklama na sociálních sítích, která upoutá vaši pozornost clickbaitovým titulkem. Jakmile na reklamu kliknete, jste přesměrováni na věrohodně vypadající článek, který pojednává o investiční příležitosti, většinou podpořené bulvárními informacemi. Pod článkem pak následuje formulář, kam mají oběti na základě pokynů útočníka zadat svoje osobní údaje. Následně se jim ozve domnělý investiční poradce. Podvod může gradovat až do podoby falešného telefonátu, tzv. vishingu, a vést k instalaci nástroje pro vzdálenou správu, čímž podvodníci získají další přístup k zařízení a datům.

„Jak můžeme vidět, kybernetické podvody se překotně vyvíjejí, stávají se součástí větších útoků a kyberpodvodníci věnují jejich přípravě a skrytí před odhalením dost času a prostředků. Určitě nadále platí všechna doporučení, jak kyberpodvod co nejlépe odhalit a pokud možno zabránit ztrátě

dat nebo finančním škodám. Především je důležité ověřovat zdroj zpráv a komunikace. Pokud přijdou bez vyžádání, neklikejte na odkazy ani neotevírejte soubory, a k heslům přidejte vícefázové ověřování. V případě dnešních útoků pomocí technik sociálního inženýrství je už rozhodně namístě zvážit pořízení bezpečnostního softwaru, který včas upozorní na škodlivé odkazy či zablokuje spuštění škodlivých příloh," uzavírá Novotný z ESETu.

Zůstaňte v bezpečí před kybernetickými podvody:

- Věnujte pozornost příchozí komunikaci, obzvlášť, pokud přijde bez vyžádání či se po vás chce nestandardní reakce. V takovém případě nikdy ve zprávě neklikejte na odkazy a nestahujte přiložené soubory. Pravdivost zprávy si nejlépe ověřte.
- Buďte obezřetní v případě různých vyskakovacích oken na webových stránkách. Jedná se o nějakou velmi pozitivní nebo naopak negativní informaci? Na jakou stránku jste po kliknutí na tlačítko s odkazem byli přesměrováni? Je URL adresa těchto stránek legitimní? Nikdy neposkytujte své osobní informace webovým stránkám, pokud si nejste jistí jejich pravdivostí.
- Pokud po vás protistrana požaduje platbu předem, vždy zbystřete. Ideálně nikdy nic neplaťte dopředu a volte vždy prověřené a osvědčené postupy předání a doručení zboží.
- U nákupu a prodeje zboží se zájemce či prodávajícího doptávejte na podrobné informace a všímejte si nejasností či chyb v komunikaci. Pokud se vám něco nezdá, komunikaci ihned ukončete.
- Nikdy nesdělujte po telefonu své osobní a citlivé informace, zejména ke svým bankovním účtům a platebním kartám. Pokud se volající představí jako pracovník banky či policie, vysvětlete mu své obavy ohledně pravdivosti hovoru a domluvte se s ním, že se spojíte s danou institucí jinou, oficiální cestou.
- Pokud po vás chce volající instalovat do zařízení nějaký software, typicky pro vzdálenou správu zařízení, odmítněte a zavěste.
- Phishingové útoky mohou otevírat dveře závažnějším kybernetickým incidentům. Nepodceňujte ochranu profesionálním bezpečnostním softwarem.
- Vytvářejte silná hesla ke svým účtům. Dbejte na pravidlo jednoho unikátního hesla pro každý účet.
- Bezpečnost hesel doplňte dalším faktorem všude tam, kde je to možné. Zpravidla se jedná o kód z SMS či spárované autentizační aplikace.

Nejčastější případy phishingových útoků v Česku za období od dubna do června 2026:

1. HTML/Phishing.Agent.HVI trojan (50 %)

Skrytý (obfuskovaný) typ phishingu s globálním dosahem, cílem jsou přihlašovací údaje, čísla kreditních karet apod.

2. HTML/Phishing.Gen trojan (29 %)

Phishingový útok s globálním dosahem, cílem jsou přihlašovací údaje, čísla kreditních karet apod.

3. HTML/Phishing.Agent.B trojan (8 %)

Podvodné webové stránky (různé oblasti).

4. HTML/Phishing.Agent.GFH trojan (4 %)

Falešné zprávy s informacemi o doručení balíčků od známých přepravců, cílem je získat peníze

z bankovních účtů obětí.

5. HTML/Phishing.Telekopye.A trojan (2 %)

Útoky pomocí nástroje Telekopye (Telekopí) s cílem získat peníze z bankovních účtů obětí.

Uživatelé a uživatelky bezpečnostních řešení od ESET jsou před těmito hrozbami chráněni.

O společnosti ESET

Společnost ESET®, která byla založena v Evropě, je předním dodavatelem řešení kybernetické bezpečnosti s pobočkami po celém světě. Poskytuje špičková řešení kybernetické bezpečnosti, která pomáhají předcházet útokům ještě před jejich vznikem. ESET kombinuje technologie umělé inteligence (AI) a lidskou odbornost, čímž pomáhá předejít nově vznikajícím globálním kybernetickým hrozbám, ať již známým či dosud neznámým. Poskytuje zabezpečení pro firmy, kritickou infrastrukturu a jednotlivce. Ať už jde o ochranu koncových zařízení, cloudu nebo mobilních zařízení, řešení a služby společnosti ESET, které využívají technologie umělé inteligence a kladou důraz na cloudové prostředí, zůstávají vysoce efektivní s minimálními nároky na uživatele.

Technologie ESET jsou vyvíjeny v EU a zahrnují robustní systém detekce a reakce, ultra-bezpečné šifrování a multifaktorovou autentizaci. S nepřetržitou obranou v reálném čase a silnou místní podporou udržuje ESET uživatele v bezpečí a firmy v chodu bez narušení jejich provozu. Neustále se vyvíjející digitální prostředí vyžaduje progresivní přístup k bezpečnosti. Jen v České republice nalezneme tři výzkumná a vývojová centra společnosti, a to v Praze, Jablonci nad Nisou a Brně. Výzkumné pobočky po celém světě podporují aktivity společnosti v rámci Threat Intelligence, stejně jako její silná globální síť partnerů.

Více informací

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost naleznete například v online magazínu Dvojklik.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide. Nejčastějším rizikům pro děti na internetu se věnuje iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET, v podcastu RESET a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

Lucie Mudráková
Specialistka PR a komunikace
ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.com

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.
tel: +420 720 829 561
vitezslav.pelc@eset.com

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/falesne-vyhry-zablokovane-ucty-i-pokuty-soucasti-kyberpodvodu-v-cesku-byly-ve-druhem-ctvrtleti-online-reklamy