Kyberpodvody v Česku: Nejčastěji se v prvním čtvrtletí útočilo na naše hesla, vrátilo se i falešné hlasování na WhatsApp

28.4.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

V prvním čtvrtletí letošního roku v Česku jednoznačně převládaly kybernetické podvody určené k získání přihlašovacích údajů. Aby útočníci tohoto cíle dosáhli, zneužívali nadále celou řadu známých služeb a společností. Vyplývá to z analýzy phishingových útoků na Českou republiku od společnosti ESET za období od ledna do března 2026. Ve sledovaném období dále opět narostly případy podvodů na chatovací platformě WhatsApp. Bezpečnostní experti z ESETu také nadále sledují propracované investiční podvody Nomani, při kterých útočníci pomocí nástrojů umělé inteligence zneužívají tváře českých politiků a celebrit.

Ve dvou třetinách všech sledovaných phishingových útoků v Česku se v prvním čtvrtletí nejvíce objevovala podvodná komunikace zacílená na krádež našich přihlašovacích údajů. Stejně jako v předchozím sledovaném období, i tentokrát byl jejím hlavním zdrojem e-mail.

„Zatímco ještě na konci loňského roku se podvody zacílené na naše přihlašovací údaje nebo čísla platebních karet, které monitorujeme pod označením Phishing.Gen, objevovaly v necelé polovině všech zachycených phishingových útoků, v období od ledna do března 2026 jsme je pozorovali již ve dvou třetinách všech případů. Hlavním zdrojem této podvodné a manipulativní komunikace byl opět e-mail. Tento typ podvodů se ale velmi často šíří i prostřednictvím reklam na sociálních sítích," připomíná Ondřej Novotný, kyberbezpečnostní analytik z pražské výzkumné pobočky společnosti ESET.

Kybernetické podvody označené jako Phishing.Gen v prvním čtvrtletí výrazně převážily nad ostatními typy phishingových útoků v Česku. Útočníci je cílí globálně a komunikaci vydávají za zprávy od celé řady firem a značek. Proto ani komunikace v angličtině nemusí na první pohled vzbudit na straně uživatelů a uživatelek podezření.

„Útočníci v těchto případech velmi často zneužívají jméno přepravce DPD, platformy Facebook nebo telekomunikačních společností, například O2. Zpráva anebo inzerce obsahuje falešný odkaz nebo dokonce QR kód k přihlášení do uživatelského účtu. Jakmile oběť na odkaz klikne, je přesměrována na falešné webové stránky s přihlašovacím formulářem. Své cenné údaje pak útočníkům sama předá," vysvětluje Novotný.

Kyberbezpečnostní experti z ESETu nadále sledují také vývoj investičních podvodů v Česku. Tento typ útoků označují názvem Nomani. Zpravidla se jedná o podvodné investice do kryptoměn. Podvodníci k jejich přípravě využívají nástroje umělé inteligence a jejich součástí je tzv. deepfake. Obvykle se jedná o upravenou fotografii nějaké známé osobnosti, ať už z řad politiků nebo celebrit.

„Ačkoli v našich analýzách vidíme, že počet investičních podvodů je zhruba na úrovni loňského jara a oproti druhému i třetímu kvartálu loňského roku klesá, jedná se aktuálně o jeden z nejrozšířenějších podvodů v České republice. Útočníci jej provádějí v několika dějstvích a pro oběti mohou představovat opravdu značné finanční ztráty, než je odhalí. Začínají prakticky vždy 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 nějaké investiční příležitosti, většinou podpořené nějakými bulvárními informacemi ze světa politiky nebo

celebrit. Útočníci v těchto případech například dlouhodobě zneužívají postavu současného českého premiéra Andreje Babiše. Pod článkem pak následuje formulář, do kterého mají podvodníkem instruované oběti zadat svoje osobní údaje. Následně se jim ozve domnělý investiční poradce a podvod se naplno může rozjet," varuje Novotný.

Nomani je typ podvodu, který kombinuje několik různých technik sociálního inženýrství, včetně tzv. vishingu. Útočníci mohou své oběti po telefonu vyzvat i k instalaci nástroje pro vzdálenou správu, čímž získají další přístup k jejich zařízení, datům a mohou tak pokračovat v manipulativní komunikaci.

Zatímco na konci loňského roku se útočníci stojící za podvody s odcizením účtu na komunikační platformě WhatsApp trochu odmlčeli, hned v prvním čtvrtletí se vrátili s novou vlnou těchto útoků. Jejich cílem je přes falešnou výzvu k hlasování získat kontrolu nad vaším účtem a následně ho zneužít k rozesílání podvodné komunikace na vaše kontakty. Podvod je zákeřný tím, že výzva k hlasování může přijít zdánlivě od někoho z vašich přátel nebo dokonce členů rodiny. Útočníci také sázejí na jistotu – aplikace WhatsApp je s přehledem nejoblíbenější chatovací platformou, kterou v Česku používáme.

„Jakmile se rozhodnete hlasovat, po kliknutí na škodlivý odkaz se ocitnete na stránce, kde musíte ale pro uskutečnění hlasování ověřit svou totožnost. Vyplníte tedy své telefonní číslo, což už zároveň vidí i podvodník, který jej tímto způsobem získá. Pro ovládnutí přístupu k vašemu účtu potřebuje ještě ale potvrzovací kód. Falešná hlasovací webová stránka vás tedy ještě jednou vyzve k dokončení ověření vaší identity zadáním tohoto kódu – a ten opět uvidí útočník. Pak již snadno může ovládat váš účet a požádat vaše příbuzné třeba o finanční půjčku," vysvětluje Novotný z ESETu.

Bezpečnostní experti radí v případě, že se stanete obětí tohoto podvodu, co nejdříve odebrat v nastavení svého účtu zařízení podvodníka. Dalším bezpečnostním opatřením může být aplikaci zcela odinstalovat a při opětovném nastavení posílit její bezpečnost přidáním dvoufaktorového ověření.

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

Phishingový útok zaměřený na krádež účtu na WhatsApp a následné rozesílání falešných zpráv.

Podvodné webové stránky (různé oblasti).

Phishingový útok s globálním dosahem, cílem jsou přihlašovací údaje.

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

Uživatelé bezpečnostních řešení od ESET jsou před těmito hrozbami chráněni.

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 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/kyberpodvody-v-cesku-nejcasteji-se-v-prvnim-ctvrtleti-utocilo-na-nase-hesla-vratilo-se-i-falesne-hlasovani-na-whatsapp