Kyberpodvody v Česku: Koncem roku se podvody nejvíce šířily přes e-mail, útočníci chtěli hlavně naše přihlašovací údaje

3.2.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Česko bylo závěrem roku 2025 cílem globálních kyberpodvodů, ve kterých útočníci zneužívali jména celosvětově známých služeb. V českém prostředí se lidé mohli setkat i s falešnými webovými stránkami telekomunikačních společností nebo bank. Vyplývá to z analýzy phishingových útoků na Českou republiku od společnosti ESET za poslední čtvrtletí roku 2025. Cílem útočníků byly na konci roku především přihlašovací údaje a k distribuci podvodných zpráv nejvíce využívali e-mail. Rizikem v Česku zůstaly koncem roku také podvody na internetových bazarech.

„Zatímco na podzim jsme v Česku pozorovali ještě určitý pokles phishingových útoků, v posledním čtvrtletí roku 2025 nabrala podvodná komunikace opět na síle. Nejčastější případy podvodných zpráv zůstávají zatím stále stejné, což svědčí o určité úspěšnosti těchto útoků: k odcizení přihlašovacích údajů útočníci využívají především e-mail, nebo také reklamy na sociálních sítích. Útok je zacílen globálně, takže se zpráva může tvářit jako komunikace od celé řady společností – velmi často je zneužívané jméno přepravce DPD, platformy Facebook nebo telekomunikačních společností. V našem prostředí jsme viděli například podvodnou komunikaci od operátora 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," vysvětluje Ondřej Novotný, kyberbezpečnostní analytik z pražské výzkumné pobočky společnosti ESET.

Výše popsané kyberpodvody v Česku, označené bezpečnostními experty jako Phishing.Gen, jsou celosvětově rozšířeným typem hrozby. Často existují v mnoha jazykových mutacích a stále se vyznačují viditelně strojovým překladem. V posledním čtvrtletí se k nim pak přidaly také podvody, které bezpečnostní experti označují jako Agent.HEE. Útočníkům šlo i v těchto případech o přihlašovací údaje.

„Přihlašovací údaje se závěrem loňského roku staly evidentně nejčastěji vyhledávanou kořistí v českém kyberprostoru. Také ve druhém, nejčastěji zachyceném podvodu hrál stěžejní roli e-mail jako způsob distribuce falešné komunikace a odkazů. Útočníci zneužívali v komunikaci přihlášení ke službě Gmail od Google či do účtu Microsoft. Manipulativní zpráva se oběti snažila vystrašit bezpečnostním upozorněním, že s účtem není vše v pořádku a vyzývala k otevření dokumentu PDF, Word či Excel prostřednictvím vloženého odkazu. I v tomto případě však byli lidé přesměrováni na podvodné stránky s falešnými přihlašovacími formuláři. V českém prostředí se mohli uživatelé setkat s verzí zneužívající Českou spořitelnu," doplňuje Novotný.

V aktuálním roce bezpečnostní experti počítají s tím, že úspěšné scénáře budou útočníci nadále zdokonalovat. Významnou součástí dnešních phishingových útoků jsou také nástroje umělé inteligence, které dokážou přizpůsobit podvodnou komunikaci na míru cílové skupině potenciálních obětí. Bezpečnostní experti tak očekávají další nárůst vysoce kvalitních deepfakes a podvodů generovaných AI, které umožní i méně zdatným útočníkům provádět masivní kampaně.

Podvod jako součást nákupů na online bazarech

Mezi nejčastějšími případy podvodů v Česku zůstávají nadále také podvody pomocí nástroje Telekopí (Telekopye). Doménou útočníků jsou v těchto případech především online tržiště a bazary. Zatímco ve třetím čtvrtletí loňského roku zachytili bezpečnostní experti tento typ podvodu v pětině všech phishingových útoků na Česko, v závěru roku klesl jejich objem na desetinu všech těchto útoků. Cílem podvodníků jsou údaje z našich platebních karet či přístupy k našim bankovním účtům.

„Nástroj Telekopí funguje jako bot v rámci komunikační platformy Telegram. Umožňuje i méně technicky zdatným útočníkům vytvářet phishingové stránky z přednastavených šablon, generovat škodlivé QR kódy a falešné screenshoty nebo rozesílat podvodné e-maily či SMS zprávy. Útočníkům připraví věrohodně vypadající, nicméně falešné kopie platebních bran na domnělých stránkách známých dopravců, jako je například DPD. Útočník si oběť typicky vybere mezi prodávajícími, předstírá zájem o prodávané zboží a následně oběti nabídne možnost platby zadáním údajů k jeho platební kartě či účtu. Právě tento postup by měl uživatele a uživatelky vždy varovat – pokud jsou v pozici prodávajícího, nedává smysl, aby někam zadávali údaje ke své platební kartě," opakuje doporučení Novotný.

Investiční podvody v závěru roku 2025

V závěru loňského roku se investiční podvody, které bezpečnostní experti z ESETu monitorují pod označením HTML/Nomani, vrátily opět blíž k hodnotám ze začátku roku. Podvody slibující pohádkové zhodnocení financí nákupem kryptoměn tak zůstávají významnou hrozbou pro české uživatele a uživatelky. Přispívá tomu i to, že útočníci v jejich případech využívají zmanipulovaný deepfake obsah.

„V loňském roce vzrostly případy podvodů Nomani v našich datech meziročně o 62 % a v souvislosti s nimi za celý rok ESET zablokoval přes 64 000 webových URL adres. Jedná se o podvod, který kombinuje několik různých technik sociálního inženýrství. U investičních podvodů lidem opakovaně připomínáme, aby zbystřili vždy, když je nabídka zhodnocení příliš výhodná a lákavá. Většinou to totiž není pravda," varuje Novotný a dodává: „Na podvody typu Nomani narazíte typicky na sociálních sítích, nejdříve v podobě nějaké chytlavé reklamy s clickbaitovým titulkem. Po kliknutí jste přesměrováni na falešný web s formulářem pro zadání vašich údajů. Následuje vishingový telefonní hovor s falešným poradcem, který vás má přemluvit do prvního investičního vkladu. Pokud své peníze pošlete, dochází postupně k navyšování částek, nátlaku k půjčce či k instalaci nástroje pro vzdálený přístup do vašeho zařízení. Pokud se pokusíte o výběr zisku, podvodníci se zpravidla nadobro odmlčí a vy své peníze již nikdy neuvidíte," dodává 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.
- 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.

- 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 října do prosince 2025:

Phishingový útok s globálním dosahem, cílem jsou přihlašovací údaje.

Phishingový útok s globálním dosahem, cílem jsou přihlašovací údaje.

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

Phishingový útok na bankovní údaje českých uživatelů a uživatelek.

Phishing zneužívající varování o expiraci předplatného za webový hosting, cílem jsou platební údaje.

Uživatelé produktů 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-koncem-roku-se-podvody-nejvice-sirily-pres-e-mail-utocnici-chteli-hlavne-nase-prihlasovaci-udaje