AI podvody sú presvedčivé: Stačí jeden klik a podvodník získa tisíce eur. Ako znížiť riziko?

8.9.2026 - Lenka Ivančíková | Zajtra studio spol.

Internetové podvody sa neustále vyvíjajú a útočníci čoraz viac stavajú na manipulovaní ľudí. Namiesto snahy prelomiť bezpečnostné mechanizmy sa pokúšajú presvedčiť obete, aby peniaze poslali sami. Využívajú pritom telefonáty, SMS správy, e-maily, sociálne siete a čoraz častejšie aj nástroje umelej inteligencie. Snažia sa dostať obeť pod psychický tlak, časovú tieseň a vyvolať v nej pocit ohrozenia.

Na aktuálne trendy upozornili **VÚB banka** a kyberbezpečnostná spoločnosť **ESET**. Ich údaje ukazujú, že medzi najčastejšie hrozby patria investičné podvody, falošné telefonáty, phishing v rôznych formách, NFC útoky či vydieračské sextortion správy.

Zdroj: Lenka Ivančíková

Útočníci chcú, aby obeť poslala peniaze sama

Podľa správy VÚB banky sa podvodníci postupne presúvajú **od krádeže údajov k priamej manipulácii klienta**. Presvedčiť človeka, aby vykonal platbu, môže byť totiž jednoduchšie než prekonať ochranné mechanizmy banky.

Problémom je, že takéto podvody sa horšie odhaľujú. Ak klient transakciu sám potvrdí a pri následnom preverovaní neuvedie pravý dôvod platby, banka má menej možností zasiahnuť. **Na vine býva pocit hanby** z vlastného zlyhania. To ale nie je na mieste. Naletieť môže naozaj každý, aj technicky zdatný človek alebo dokonca ten, kto sa kyberbezpečnosťou profesne zaoberá. Stačí, že je unavený, pod tlakom, a tak klikne aj na odkaz, pri ktorom by za bežných okolností spozornel.

Podvodníci sa vydávajú napríklad za pracovníkov banky, policajtov, pracovníkov finančnej správy alebo rodinných príslušníkov v núdzi. Na kontaktovanie obetí používajú prakticky všetky bežné komunikačné kanály. Nielen telefonáty a maily, ale aj SMS-ky, Messenger i WhatsApp.

Zdroj: VÚB

Najviac prípadov sa týka ľudí nad 61 rokov

Z údajov VÚB vyplýva, že **najohrozenejšou skupinou sú ľudia vo veku nad 61 rokov**. Kým v roku 2025 bolo najviac podvedených vo veku 61 až 66 rokov, v roku 2026 sa k nim počtom prípadov približuje aj skupina vo veku 67 až 71 rokov.

Veľkým problémom sú najmä **falošné investície**. Priemerný vek podvedených pri tomto type útoku je 63 rokov a **priemerná strata presahuje 2 000 eur**. Vzhľadom na vysoký počet prípadov ide zároveň o kategóriu s najvyšším celkovým objemom finančných strát.

Ešte vyššiu škodu však môže spôsobiť podvodný telefonát. Falošný policajt alebo údajný pracovník NBS **pripravil v priemere jednu obeť o viac než 7 250 eur**. Najvyššia individuálna strata podľa údajov banky dosiahla **až 115-tisíc eur**.

Zdroj: VÚB

Pribúda aj NFC tunneling

Do pozornosti sa dostáva aj technika označovaná ako NFC tunneling. Ide o **zneužitie NFC komunikácie platobnej karty**, po ktorom môže nasledovať neoprávnený výber z bankomatu.

Podvodníci pritom opäť používajú sociálne inžinierstvo. Ako zámienku môžu spomenúť napríklad vyplatenie údajného výnosu z investície a následne obeť navedú k ďalším krokom.

Sextortion e-maily dokážu zarobiť milióny

ESET upozorňuje aj na výrazný nárast sextortion správ. Ide o vydieračské e-maily, v ktorých útočník tvrdí, že získal prístup k zariadeniu alebo webkamere obete a disponuje kompromitujúcim obsahom z prezerania obsahu určeného dospelým. Za jeho nezverejnenie potom požaduje platbu, často v bitcoinoch.

Samotný podvod môže pôsobiť jednoducho a väčšina príjemcov mu neuverí. Pri masovom rozosielaní však aj malé percento úspešných prípadov môže priniesť vysoké zisky.

Zdroj: Lenka Ivančíková

ESET analyzoval vzorku 3,5 milióna škodlivých e-mailov zozbieraných medzi marcom a augustom 2026. Analytici získali tisíce bitcoinových adries používaných na vydieranie minimálne od roku 2017. Na približne tisícke sledovaných peňaženiek sa **v období rokov 2017 až 2026 uskutočnili transakcie v objeme 321 bitcoinov**, čo ESET pri konzervatívnom prepočte vyčíslil približne na **3,5 milióna eur**.

Medzi prvou a druhou polovicou roka 2026 podľa telemetrie ESETu narástol počet sextortion e-mailov o 36 %. Ak by trend pokračoval, celoročný nárast by mohol dosiahnuť až 170 %.

Phishing stále patrí medzi najčastejšie hrozby

Sextortion pritom ESET nezaraďuje priamo medzi phishing. Ten má za cieľ získať prihlasovacie, platobné alebo iné citlivé údaje a tvorí približne každú piatu hrozbu zachytenú v telemetrii spoločnosti. Pod phishing patria nielen e-maily, ale aj podvodné SMS správy, správy v chatovacích aplikáciách či škodlivé QR kódy.

Zdroj: Lenka Ivančíková

Často sa kombinuje aj so škodlivým softvérom. ESET upozorňuje napríklad na hrozbu **CloudEyE**, ktorá sa zameriava aj na používateľov v strednej Európe a na Slovensku. Jej úlohou je dostať do zariadenia ďalší malvér.

Len počas prvých šiestich mesiacov roka 2026 zaznamenal ESET pri CloudEyE **rast takmer o 190 %**. K infekcii môže podľa spoločnosti stačiť otvorenie falošnej faktúry alebo reakcia na kvalitne podvrhnutý e-mail.

AI pomáha vytvárať presvedčivejšie podvody

Umelá inteligencia podvodníkom uľahčuje tvorbu obsahu, ktorý môže pôsobiť dôveryhodnejšie. Môže ísť o napodobnenie hlasu blízkej osoby, falošné dokumenty alebo deepfake videá.

AI sa používa aj pri investičných podvodoch. ESET sleduje kampane označované ako **Nomani**, ktoré využívajú falošné investičné platformy a často aj deepfake obsah. V roku 2026 spoločnosť zablokovala takmer 50-tisíc URL adries prepojených s týmito kampaňami.

Zdroj: Lenka Ivančíková

Útočníci podľa ESETu využívajú AI nielen pri tvorbe reklám a videí, ale aj na generovanie nových falošných webov či presvedčivo pôsobiacich recenzií.

Najprudší rast kampaní Nomani zaznamenal ESET medzi rokmi 2024 a 2025, keď išlo o nárast 113 %. Po následnom poklese aktivity sa útoky od júna 2026 opäť zintenzívnili. Ak by tento trend pokračoval do konca roka, polročný rast detekcií by mohol dosiahnuť približne 30 %.

Ako znížiť riziko podvodu

Najdôležitejšou ochranou zostáva overovanie informácií. Peniaze by ste nemali posielať iba na základe telefonátu, SMS alebo správy v komunikačnej aplikácii. Ak vás niekto tlačí do rýchleho rozhodnutia, je vhodné komunikáciu prerušiť a kontaktovať banku, firmu alebo blízku osobu cez nezávislý kanál.

Do telefónu alebo počítača si neinštalujte neznáme aplikácie ani nástroje na vzdialený prístup na pokyn cudzej osoby. Pozorne si čítajte autorizačné správy z banky a nikdy neposkytujte prihlasovacie údaje, autorizačné kódy či údaje z platobnej karty.

Zdroj: Lenka Ivančíková

Mohlo by vás zaujímať:

- Windows 11 dostane praktický widget. Na jednom mieste ukáže stav batérie všetkých zariadení
- Oura priznala problém s batériou prsteňa Ring 4. Záruky ju stáli milióny dolárov
- Nothing OS 5.0 prinesie veľkú dávku noviniek. Ktoré smartfóny ho dostanú?

Dôležité sú aj pravidelné aktualizácie systému (mobil aj PC) a aplikácií, silné heslá alebo passkeys a bezpečnostné riešenie. Pri nečakanej správe či výhodnej investičnej ponuke sa oplatí skontrolovať adresu odkazu, odosielateľa a celý obsah overiť ešte z iného zdroja.

Zdroj: Lenka Ivančíková

Podvodníci dnes čoraz častejšie neútočia priamo na technológie, ale na človeka pred obrazovkou. S nástupom AI pritom môže byť stále náročnejšie rozpoznať, či hlas, video alebo správa pochádza od osoby, za ktorú sa vydáva. **Nezabudnite:** ak ste sa stali obeťou podvodu, hanba musí ísť bokom. Treba kontaktovať banku, prípadne políciu, lebo len tak je šanca na zvrátanie podvodnej platby a získania aspoň časti peňazí späť.

https://www.mojandroid.sk/ai-podvody-su-presvedcive-staci-jeden-klik-a-podvodnik-ziska-tisice-eur-ako-znizit-riziko