E-šmejdi přitvrzují: Komerční banka varuje před novou vlnou podvodů

26.3.2026 - | Komerční banka

Kybernetická kriminalita v České republice sílí a „e-šmejdi“ neustále zdokonalují své metody, jak se dostat k úsporám klientů. Komerční banka (KB) proto upozorňuje na aktuální vlny podvodů, které zneužívají důvěru lidí v autority i jejich ochotu pomoci blízkým. Zároveň vyzývá klienty k maximální obezřetnosti a připomíná, aby využívali dostupné bezpečnostní nástroje, například ověření bankéře v mobilní aplikaci.

Jedním z nejčastějších scénářů poslední doby je tzv. **vishing**, tedy podvodné telefonáty. Útočníci dokážou pomocí techniky zvané spoofing napodobit jakékoli telefonní číslo, často například infolinku banky, policie nebo jiné instituce. Volající se pak vydává za bankéře, policistu nebo pracovníka České národní banky a tvrdí, že je účet či platební karta klienta v ohrožení. Pod záminkou „záchrany peněz“ následně oběť přesvědčí, aby své prostředky převedla na údajně bezpečný účet, který je ve skutečnosti pod kontrolou podvodníků. Další variantou tohoto podvodu je scénář, kdy útočník klienta přesvědčí, aby si do telefonu nainstaloval údajnou „bezpečnostní aplikaci“. Následně ho vyzve, aby k mobilu přiložil platební kartu a zadal PIN kvůli jejímu „ověření“ – ve skutečnosti tím však dojde k přenosu karetních údajů do podvodné aplikace a útočník může kartu zneužít například pro výběry z bankomatu nebo platby v obchodech.

„Podvodníci velmi dobře pracují s psychologií. Snaží se vyvolat strach, časový tlak a pocit, že je potřeba jednat okamžitě. Právě v takové chvíli lidé často udělají rozhodnutí, které by za běžných okolností nikdy neudělali. Klienti Komerční banky si přitom mohou volajícího bankéře snadno ověřit přímo v mobilní aplikaci KB+ – skutečný bankéř jim do ní pošle potvrzení se svým jménem. Podvodník takovou výzvu splnit nedokáže a obvykle proto po vyzvání k ověření ihned zavěsí.“

Pavel Šašek, expert na kyberbezpečnost Komerční banky

Vedle toho banka zaznamenává také další typy útoků. Patří mezi ně například falešné zprávy o **daňovém přeplatku**, které napodobují komunikaci Finanční správy a odkazují na podvodné stránky imitující portál Moje daně. Objevují se také podvodné SMS zprávy vyzývající k **urgentní aktualizaci Bankovní identity (Bank iD)**. Přibývá i případů, kdy e-šmejdi ovládnou **WhatsApp profil**. Z toho pak rozesílají zprávy, které vyzývají k hlasování v různých soutěžích nebo k podpoře údajné „talentované dívky“. Odkaz ve zprávě vede na falešnou stránku, přes kterou útočníci získají plnou kontrolu nad WhatsApp účtem oběti. Následně jejím jménem oslovují uložené kontakty a snaží se od nich vylákat peníze například prostřednictvím žádosti o rychlou půjčku.

„Scénáře podvodů se neustále vyvíjejí a útočníci se snaží reagovat na aktuální situace – například na daňovou sezonu nebo nové digitální služby. Základní pravidlo ale zůstává stejné: banka ani policie po klientech nikdy nepožadují hesla, PIN kódy ani převody peněz na jiné účty,“ dodává Pavel Šašek.

Jak se nenechat e-šmejdy oklamat:

- **Využívejte ověření v aplikaci**: Je to nejrychlejší cesta, jak v reálném čase poznat podvodníka od skutečného bankéře.

- **Nereagujte na výzvy k převodu peněz:** Banky nikdy nevyžadují převod prostředků na „bezpečné účty“.
- **Prověřujte adresy webů:** Oficiální doména pro Bank iD je pouze bankid.cz, pro Finanční správu pak financnisprava.gov.cz.
- **Chraňte své kódy a hesla:** Nikdy nikomu nesdělujte ani nepřeposílejte autorizační SMS kódy, PINy ani hesla k bankovnictví.
- **Ověřujte si zprávy od přátel**: Pokud vás někdo blízký na WhatsAppu žádá o peníze, zavolejte mu standardním telefonním hovorem, abyste si potvrdili jeho identitu.

V případě podezření na podvodné jednání hovor okamžitě ukončete a kontaktujte oficiální klientskou linku KB na čísle **+420 955 551 505** nebo linku pro blokaci karet.

https://www.kb.cz/cs/o-bance/tiskove-zpravy/e-smejdi-pritvrzuji-komercni-banka-varuje-pred-novou-vlnou-podvodu