E-šmejdi přitvrzují: počet podvodů vzrostl o více než třetinu, pro hotovost si posílají kurýry

5.8.2026 - | Komerční banka

Komerční banka zaznamenala v prvním pololetí letošního roku v oblasti plateb a platebních karet přibližně o 41 % více podvodů než ve stejném období roku 2025. Současně se jí podařilo klientům zachránit peníze v objemu několika stovek milionů korun. Vedle investičních podvodů, phishingu a falešných bankéřů se stále častěji objevují také nové nebo výrazně upravené scénáře. Podvodníci si pro vybranou hotovost posílají kurýry, zneužívají skutečné rezervace ubytování nebo klienty přesvědčují, aby si nainstalovali falešnou bankovní aplikaci a přiložili k telefonu svou platební kartu.

Růst kyberpodvodů nepolevuje. Data Komerční banky za první pololetí roku 2026 ukazují, že počet napadených platebních karet se meziročně zvýšil o 33 % a hodnota podvodných karetních transakcí vzrostla o 80 %. V oblasti platebního styku přibylo 49 % napadených klientů a hodnota podvodných transakcí se více než zdvojnásobila. Nejčastějšími platebními podvody zůstávají investiční a krypto podvody, které představují 48 % celkové hodnoty podvodných transakcí, následované vishingem, tedy falešnými telefonáty bankéřů nebo policistů, s podílem 39 %. U platebních karet stojí za 61 % případů phishing.

„Za první pololetí jsme klientům zachránili několik set milionů korun. Současně ale vidíme, že počet případů i způsobené škody dál rostou a útočníci své scénáře velmi rychle obměňují. Když se lidé naučí odmítat převod na údajně bezpečný účet, podvodník pošle kurýra pro hotovost. Když znají funkci ověření bankéře v aplikaci, snaží se jim e-šmejdi namluvit, že kód zaslaný přes SMS nebo WhatsApp je totéž. Proto musíme vedle technologií průběžně měnit také způsob, jakým klienty před aktuálními hrozbami varujeme.“

Pavel Šašek, expert na kyberbezpečnost Komerční banky

Nové scénáře jsou úspěšné především proto, že technické znalosti ani inteligence člověka v takové situaci nehrají rozhodující roli. *„Podvodníci využívají přirozené fungování lidského mozku při akutním stresu. Nejprve vyvolají pocit ohrožení nebo hrozící ztráty a tím spustí silnou emoční a stresovou reakci. Následně vytvoří časový tlak, vystupují jako autorita a člověka postupně izolují od lidí i informací, které by mu pomohly situaci racionálně vyhodnotit. Mozek se v takové chvíli přirozeně soustředí především na co nejrychlejší odstranění bezprostředně vnímané hrozby - nikoliv na důkladné ověřování informací. Dochází ke zúžení pozornosti, člověk hůře vnímá souvislosti, obtížněji zvažuje alternativy a snáze přehlédne varovné signály. Nejde tedy o hloupost ani nedostatek zkušeností. Jde o běžnou reakci mozku na akutní stres, kterou může za určitých okolností zažít každý z nás,“* vysvětluje psycholožka Helena Sováková, která více než dvacet let působila v ozbrojených složkách a vedla Odbor operační psychologie Armády České republiky.

Právě proto musí ochrana klientů kombinovat technologie s rychlou reakcí a prevencí. Komerční banka denně analyzuje přibližně 1,2 milionu karetních transakcí, 600 tisíc plateb a zhruba jeden milion nefinančních operací v digitálních kanálech. Její expertní tým pracuje v režimu 24/7 a při vyhodnocování rizik využívá více než 300 detekčních pravidel, historii chování klienta, lokalitu, IP

adresy a další údaje.

Od „bezpečného účtu“ k obálce předané na parkovišti

Jedním z výrazných trendů posledních měsíců je předávání hotovosti přímo podvodníkům. Útočník se vydává například za pracovníka banky, České národní banky, policistu nebo investičního poradce a klienta přesvědčí, že peníze musí zachránit nebo výhodně investovat. Oběť následně vybere statisíce korun z bankomatu či na pobočce a na domluveném místě je předá falešnému kurýrovi. Ten může předložit falešný průkaz, potvrzení o převzetí nebo jiný dokument, který má celé situaci dodat zdání důvěryhodnosti.

Podvodníci klientům často předem poradí, jak pracovníkům banky vysvětlit neobvykle vysoký výběr. Jako důvod mají uvést například rekonstrukci, koupi auta nebo pomoc rodině. Podvodník tím oběť nejen připravuje na otázky bankéře, ale zároveň ji izoluje od člověka, který by mohl celý příběh zpochybnit. Jakmile kurýr hotovost převezme, šance na její získání zpět je minimální.

Další nový scénář kombinuje vishing s falešnou aplikací a technikou označovanou jako NFC relay attack neboli „červí díra“. Podvodník klientovi oznámí, že jeho účet nebo karta jsou v ohrožení, a pošle mu odkaz na údajnou bezpečnostní aplikaci. Po její instalaci ho přiměje, aby k telefonu přiložil fyzickou platební kartu a zadal PIN, údajně kvůli ověření nebo resetu karty. Ve skutečnosti se údaje přenesou k útočníkovi, který pak může vybírat hotovost z bankomatu nebo kartou platit, jako by ji měl fyzicky u sebe.

Podvodníci se pokoušejí napodobit také službu ověření bankéře. Klientovi zašlou kód prostřednictvím SMS či WhatsAppu a tvrdí, že tím prokazují svou totožnost. Skutečné ověření pracovníka KB však probíhá výhradně v aplikaci KB+ nebo KB Klíč, kde klient vidí jméno bankéře a čtyřmístný kontrolní kód. Ověření zaslané běžnou zprávou je podvod.

Čím déle podvod trvá, tím hůř se z něj vystupuje

Podvodníci obvykle nezačínají požadavkem na převod celoživotních úspor. Nejprve chtějí malý, zdánlivě neškodný krok – například instalaci aplikace, ověření platby nebo zadání jednoho údaje. Využívají přitom přirozenou tendenci lidského mozku zachovávat soulad s předchozími rozhodnutími. Jakmile člověk udělá první krok, roste pravděpodobnost, že bude pokračovat i v dalších, protože mozek má přirozenou potřebu dokončit to, co už začal. Každé další rozhodnutí se pak opírá o to předchozí a vystoupit z celého procesu je stále obtížnější. *„Člověk už neinvestuje jen peníze, ale také svůj čas, důvěru a vlastní rozhodnutí. Přiznat si, že první krok byl chybný, je psychicky náročné, proto mozek častěji hledá důvody, proč pokračovat, než aby své předchozí rozhodnutí zpochybnil. U investičních podvodů proto může oběť posílat další peníze i ve chvíli, kdy ji banka varuje. Naděje, že ještě jedna platba vše napraví, je pro mozek v dané chvíli psychicky snesitelnější než přijmout ztrátu a připustit vlastní omyl. Právě proto je při prevenci podvodů zásadní spolupráce klienta a banky. Banka dokáže rozpoznat řadu rizikových situací a klienta včas upozornit, sama však podvod zastavit nemůže. Stejně důležité je, aby klient znal nejčastější scénáře podvodů, věděl, jak banka své klienty skutečně kontaktuje a ověřuje jejich totožnost, a dokázal tato pravidla uplatnit i ve chvíli, kdy je pod silným tlakem. Jen propojení preventivních opatření banky s informovaným rozhodováním klienta dává největší šanci podvod včas odhalit nebo alespoň výrazně zmírnit jeho následky,“* vysvětluje psycholožka Helena Sováková.

Významnou roli hraje také stud. Poškození se mohou obávat reakce rodiny, okolí nebo policie, a proto podvod neoznámí okamžitě. Útočník tím získává další čas na výběr nebo převedení peněz. Čím dříve klient banku kontaktuje, tím větší je šance, že se podaří alespoň část prostředků zachránit.

Letní dovolená jako ideální příležitost

V období dovolených přibývá podvodů spojených s rezervací ubytování, auta nebo dalších cestovních služeb. Útočníci mohou znát konkrétní údaje o rezervaci, a jejich zpráva proto působí mimořádně důvěryhodně. Vydávají se za hotel nebo zákaznickou podporu rezervačního portálu a tvrdí, že platba neproběhla, je nutné ověřit kartu nebo doplatit městský poplatek, servisní poplatek či vratnou kauci.

Falešná výzva může přijít e-mailem, SMS, přes WhatsApp, ale také prostřednictvím interního chatu samotného rezervačního portálu. Odkaz pak klienta zavede na stránku, která vzhledem napodobuje skutečný rezervační systém, ale slouží k získání karetních nebo osobních údajů. *„Tyto podvody jsou nebezpečné tím, že útočníci mohou pracovat se skutečnými údaji o rezervaci, takže zpráva působí velmi věrohodně. Varovným signálem je tlak na rychlou platbu, hrozba zrušením rezervace nebo požadavek, aby klient znovu zadal údaje ke kartě prostřednictvím zaslaného odkazu. V takové situaci doporučujeme komunikaci přerušit a vše ověřit přímo v oficiální aplikaci, na webu rezervační služby nebo u konkrétního ubytovacího zařízení,“* upozorňuje Pavel Šašek, expert na kyberbezpečnost Komerční banky.

Falešná rodina, e-shopy i investice

Nadále se šíří také podvody prostřednictvím aplikace WhatsApp. Útočník ovládne cizí profil a jeho jménem osloví rodinu nebo přátele například s žádostí o rychlou půjčku na řešení údajné nouzové situace. Zpráva může obsahovat správné jméno, fotografii i informace převzaté z předchozí komunikace. Podobné žádosti je proto nutné ověřit běžným telefonátem na známé číslo. Zároveň je vhodné pravidelně kontrolovat seznam propojených zařízení v nastavení aplikace a odhlásit všechna, která uživatel nepoznává.

Velmi časté zůstávají falešné e-shopy a reklamy na sociálních sítích, které nabízejí výrazně zlevněné zboží nebo tzv. mystery boxy za několik eur. Jejich cílem často není pouze jednorázová platba za neexistující zboží, ale získání kompletních údajů k platební kartě. Komerční banka takových falešných obchodů blokuje desítky až stovky měsíčně.

Největší finanční ztráty ale nadále způsobují investiční a krypto podvody. Oběť vidí falešné grafy, zdánlivě rostoucí výnosy a často má k dispozici i osobního „poradce“. Peníze však nesměřují na její investiční účet, ale k podvodníkům. Ti klienta postupně přesvědčují k vyšším vkladům, někdy dokonce k uzavření úvěru.

„Ať už jde o zprávu od známého, podezřele výhodný nákup nebo investiční nabídku, podvodníci spoléhají na to, že člověk zareaguje rychle a bez ověření. U WhatsAppu je proto důležité žádost potvrdit telefonátem a pravidelně kontrolovat propojená zařízení. U e-shopů by měla varovat nápadně nízká cena a u investic slib vysokého výnosu bez rizika nebo tlak na okamžité rozhodnutí. Jakmile nás někdo nutí jednat ihned, měli bychom naopak zpomalit.“

Pavel Šašek, expert na kyberbezpečnost Komerční banky

Jak podvodníkovi vzít jeho největší výhodu

Komerční banka doporučuje při každé nečekané žádosti o peníze, instalaci aplikace nebo sdělení citlivých údajů komunikaci přerušit a situaci ověřit nezávislou cestou. Banka ani policie nikdy nepožadují převod peněz na „bezpečný účet“, předání hotovosti kurýrovi ani instalaci aplikace zaslané během telefonátu. Je dobré uvědomit si, co po nás volající požaduje. Není žádný jiný bezpečný účet než právě ten, který má klient ve své bance a má ho pod svým dohledem. Pokud někdo nabízí rychlé a vysoké zhodnocení financí, je dobré se před posláním peněz podívat na trh a porovnat reálnost nabídky. Volajícího bankéře KB je možné ověřit pouze přímo v aplikaci KB+ nebo KB Klíč. Při rezervaci ubytování je vhodné platit výhradně prostřednictvím oficiální aplikace nebo webu rezervační služby, případně využít virtuální kartu s omezeným limitem. Pokud již k podvodu došlo, je nejdůležitější kontaktovat banku bez prodlení.

„Podvodníci vytvářejí časový tlak a využívají únavy i dlouhodobého stresu, ve kterém lidé fungují. Právě tehdy je důležité znovu převzít kontrolu nad vlastním rozhodováním. Nepodlehnout naléhavosti, nenechat se zastrašit a dát si čas na ověření informací. Dobrou pomůckou může být jednoduchá otázka: Rozhodla bych se stejně, kdybych na to měla ještě hodinu? Pokud je odpověď nejistá, je vždy bezpečnější komunikaci přerušit, ověřit si informace přímo u poskytovatele služby nebo se poradit s někým, komu důvěřuji. Právě těch několik minut navíc může rozhodnout o tom, zda si člověk užije dovolenou, nebo přijde o své peníze,“ uzavírá Helena Sováková.

Pokud se člověk již stane obětí podvodu, je nutné ihned vše řešit se svou bankou a Policií ČR. Klíčové je nestydět se, nic nezamlčet a pravdivě popsat, co člověk podvodníkovi umožnil nebo zaslal. Právě ostych nebo neúplnost informací často brání efektivnějšímu řešení dopadů podvodů.

Komerční banka vedle nepřetržitého monitoringu transakcí a rozvoje bezpečnostních systémů dlouhodobě investuje také do prevence a vzdělávání klientů a zaměstnanců. Prostřednictvím kampaně Kyberpříšery srozumitelně představuje nejčastější podvodné scénáře a vysvětluje, jak je včas rozpoznat.

Více na https://www.kb.cz/cs/podpora/bezpecnost

Prezentace Kyberpodvody 2026 - vývoj, trendy, psychologie obětí i e-šmejdů
3,05 MBPDF

https://www.kb.cz/cs/o-bance/tiskove-zpravy/e-smejdi-pritvrzuji-pocet-podvodu-vzrostl-o-vice-nez-tretinu-pro-hotovost-si-posilaji-kuryry