Komerční banka zachytává víc kyberútoků než dřív. E-šmejdi ale mění taktiky a přitvrzují

22.4.2026 - | Komerční banka

Komerční banka v 1. čtvrtletí roku 2026 ochránila klienty před ztrátami ve výši 235 milionu korun. Podvodníci ale přitvrzují: objem podvodných plateb vzrostl mezikvartálně o 15 %. Počet zneužitých platebních karet sice klesl (o 17 %), nicméně výrazně stoupl objem hrubých škod z podvodů na kartách, a to o 45 %. I v prvním čtvrtletí dominovaly investiční a krypto podvody (51 % objemu), následované vishingem, tedy manipulací klienta v rámci podvodného hovoru typu „bankéř" nebo „policista", které tvoří 37 % objemu zaznamenaných podvodů.

Komerční banka se neustále snaží odhalovat a zastavovat podezřelé transakce, zatímco e-šmejdi přicházejí s čím dál agresivnějšími a propracovanějšími scénáři.

„Dlouhodobě posilujeme naše technologie, monitorovací nástroje i interní procesy a organizaci tak, abychom dokázali co nejvíce podvodů zastavit ještě předtím, než klientům způsobí škodu. Data za první čtvrtletí jen potvrzují, že útočníci stále rychleji reagují na to, jak se jim banky brání, a své scénáře tomu průběžně přizpůsobují."

Pavel Šašek, expert Komerční banky na kyberbezpečnost

Komerční banka denně analyzuje z pohledu prevence podvodů přibližně 1,2 milionu karetních transakcí, 600 tisíc plateb a zhruba 1 milion nefinančních transakcí a aktivit v přímých kanálech banky. Právě kombinace pokročilých technologií, průběžného vyhodnocování rizik a specializovaných týmů umožňuje odhalovat i velmi sofistikované pokusy o podvod.

Doposud nejvyšší částka, kterou se Komerční bance podařilo klientovi ochránit, byla 20 milionů korun. Klient o ni mohl přijít kvůli podvržené faktuře, podvod se ale podařilo včas zastavit. V oblasti platebních karet pak banka včas odhalila nejvyšší podvodnou platbu za 8,89 milionu korun.

Investice, falešný bankéř i nové varianty známých triků

Nejčastějším podvodným scénářem zůstávají investiční a krypto podvody. V prvním čtvrtletí roku 2026 tvořily 47 % z celkového počtu všech zaznamenaných podvodů. Jde o nejrůznější varianty nabídek investic slibujících nadprůměrný až nereálný výnos.

„Druhým nejčastějším podvodem je vishing, tedy podvodná volání typu ‚bankéř" nebo ‚policista'. Každý čtvrtý podvod dnes začíná právě tímto telefonátem. Scénář je přitom pořád stejný: falešná autorita, tlak na rychlé rozhodnutí a klient, který v dobré víře pošle peníze přímo podvodníkovi," vysvětluje Pavel Šašek.

Podvodníci velmi rychle reagují na bezpečnostní opatření bank a své scénáře tomu přizpůsobují. V poslední době tak klientům posílají SMS nebo zprávy přes WhatsApp s kódem a přesvědčují je, že jde

o součást ověření bankéře. Jindy zneužijí i legitimní bankovní procesy, například obnovu přístupu do mobilního bankovnictví – klientovi pak skutečně přijde zpráva z banky a celý podvod působí mnohem důvěryhodněji.

Opět se vrací scénář označovaný jako „podvodná rodina“. Ten je založený na zneužití aplikace WhatsApp a následném rozesílání zpráv členům rodiny nebo blízkým přátelům s prosbou o rychlou finanční pomoc, obvykle ve formě krátkodobé půjčky v řádu nižších desítek tisíc korun.

Vedle toho se objevují i scénáře, které stojí na zneužití důvěry a emocí. Podvodníci například využívají transparentní účty, aby v klientovi vyvolali dojem, že komunikuje s důvěryhodnou a legitimní protistranou. Teprve potom manipulace pokračuje směrem k převodu větších částek na jiné účty.

Velmi častým problémem také zůstávají falešné e-shopy. Typicky jde o lákavé reklamy na sociálních sítích nabízející výrazně zlevněné zboží nebo tzv. mystery boxy za několik eur. Ve skutečnosti však útočníkovi nejde o zboží, ale o získání karetních údajů. Tyto podvody nejsou vždy tolik vidět, protože jednotlivé škody často nepůsobí dramaticky a pohybují se třeba jen v řádu desítek eur. Z pohledu banky ale jde o každodenní realitu a Komerční banka takových falešných e-shopů blokuje desítky až stovky měsíčně.

Další z nových typů podvodů je opět založen na manipulaci klienta pomocí podvodného telefonátu v kombinaci s instalací falešné aplikace do mobilního zařízení. Podvodníci se snaží přesvědčit, aby klient stáhl „aktualizaci“ bankovní aplikace a sdělil PIN ke své platební kartě a přiložili svou fyzickou (plastovou) kartu k vašemu mobilnímu telefonu. Ve skutečnosti jde o falešnou aplikaci, která do telefonu nainstaluje škodlivý software. Útočníci tak získají přístup k vaší kartě a mohou s ní vybírat hotovost nebo platit – peníze z účtu mizí během chvilky.

„To, co dříve fungovalo jako jednoduchý podvodný telefonát, dnes často přerůstá v promyšlený scénář, který pracuje s důvěrou, autoritou i časovým tlakem. Útočníci testují nové cesty, jak si klienta získat. Právě proto je tak důležité každou neobvyklou žádost o peníze nebo citlivé údaje vždy zastavit a ověřit jinou cestou.“

Pavel Šašek, expert Komerční banky na kyberbezpečnost

E-šmejdi se řídí sezónou stejně jako obchodníci

Podvodné scénáře se navíc mění podle ročního období a aktuální situace. Na začátku roku jsou typické falešné zprávy o přeplatcích nebo daňových vratkách. V období podávání daňových přiznání se objevují výzvy k doplacení daně nebo k úhradě poplatků. Letní měsíce nahrávají romantickým podvodům a falešným investičním příběhům, zatímco od konce prázdnin a na podzim se rozjíždějí falešné e-shopy, zprávy o balíčcích na cestě nebo výzvy k doplacení cla a poplatků.

Podvodníci zároveň pečlivě sledují i veřejné dění. Zneužívají témata, která právě rezonují ve společnosti nebo se objevují v médiích, od nových digitálních služeb přes daňové období až po investiční trendy.

Důležité podle Komerční banky je, že se tyto podvody netýkají jen seniorů nebo méně zkušených uživatelů. Obětí se mohou stát i lidé ve městech, vysokoškoláci nebo klienti, kteří mají o online prostředí velmi dobrý přehled. Manipulativní techniky jsou totiž stále přesvědčivější a často cílí právě na emoce, ať už jde o strach o peníze, snahu rychle jednat nebo naopak vidinu výhodného

zisku.

Technologie pomáhají, bez obezřetnosti klientů to ale nepůjde

Komerční banka je v oblasti prevence platebních a karetních podvodů dlouhodobě aktivní. Pravidelně monitoruje a vyhodnocuje podezřelé transakce, zavádí dodatečné kontrolní mechanismy a rozvíjí postupy pro včasnou identifikaci podvodných scénářů. Významnou část svých aktivit věnuje také osvětě a sdílení informací o aktuálních hrozbách.

„Prevence dnes není jen o technologiích a monitoringu transakcí. Stejně důležité je umět lidem srozumitelně vysvětlit, jak podvody fungují a na co si dát pozor. Právě proto jsme přišli i s kampaní Kyberpříšery, která upozorňuje na nejrozšířenější typy podvodů srozumitelně a bez zbytečné složitosti,“ uzavírá Pavel Šašek, expert na kyberbezpečnost Komerční banky.

Kybernetická bezpečnost

Včasné rozpoznání útoku je klíčové pro ochranu vašich financí
Více o kybernetické bezpečnosti

https://www.kb.cz/cs/o-bance/tiskove-zpravy/komercni-banka-zachytava-vic-kyberutoku-nez-driv-e-smejdi-ale-meni-taktiky-a-pritvrzuji