

Efektivita boje s kyberpodvodny roste. Komerční banka zachránila v loňském roce klientům 418 milionů korun

30.1.2024 - Tomáš Zavoral, Šárka Nevoralová, Michal Teubner | Komerční banka

Za loňský rok evidovala Komerční banka dvakrát tolik kyberpodvodů, než tomu bylo v roce 2022.

Nejčastějším typem jsou stále falešné zprávy nebo e-maily. Vzrostl také počet podvodných telefonátů (vishing), při nichž se e-šmejdi snaží zmanipulovat k údajně výhodným investicím nebo k nákupu kryptoměn. V kurzu byly také tzv. romance scam, tedy sňatkové podvody v online prostoru, nebo falešné nabídky v podobě výhry například nového telefonu a podvody v oblasti cestovního ruchu – bookingových služeb.

„Každý den prověříme tisíce transakcí platebními kartami a pokud zachytíme takovou, která vykazuje znaky pokusu o podvod, obratem kontaktujeme klienta a varujeme ho. Díky tomu se nám v loňském roce podařilo zachránit klientům přes 418 milionů korun.“

Pavel Šašek, manažer karetního servisu a prevence podvodů Komerční banky

Týmy Komerční banky zaměřené na prevenci podvodů řeší každoročně stále více útoků e-šmejdů na klienty bank.

„Česko se drží v oblasti kyberpodvodů na předních místech. Je to proto, že jsme na špičce s bankovními technologiemi a bezpečností a podvodníci si to u nás zkouší. Co bude fungovat u nás, bude fungovat i jinde. Také proto v KB neustále investujeme do nových technologií, abychom ještě více zvýšili účinnost nástrojů pro aktivní odhalování kyberpodvodů.“

Marek Macháček, expert na prevenci platebních podvodů Komerční banky

Víkendy, prázdniny nebo vánoční shon jsou pro e-šmejdy žně

Podvodníci útočí v on-line prostoru téměř nepřetržitě a každý se může stát jejich terčem. Přesto existují období, kdy je třeba být více ostražitý než obvykle. „E-šmejdi si rádi vybírají dobu, kdy jsou lidé vyčerpaní a vytížení, ať už pracovní nebo psychicky. Tradičně to bývá před Vánoci, kdy panuje shon s nákupem dárků, nebo před létem, kdy zařizujeme dovolenou a jsme ve stresu, abychom všechno stihli. Nebezpečné jsou ale i víkendy, kdy jsou lidé náchylnější a nepozornější,“ objasňuje **Marek Macháček**.

Oběti si e-šmejdi volí náhodně a cílí na všechny věkové skupiny, bez rozdílu vzdělání či pohlaví. „Nelze stanovit jednoznačný profil oběti, podvodníci to zkouší plošně, nevybírají si. Pouze pozorujeme, že snadněji se na falešný nákup kryptoměn nechávají nachytat muži z menší vesnice, ročník zhruba 1970, kteří se snaží investovat částku kolem 100 až 200 tisíc,“ dodává **Marek Macháček**.

Komerční banka je velmi úspěšná v odhalování a prevenci kyberpodvodů. Denně prověří zhruba půl milionu transakcí a v případě podezření na podvod, klienta obratem kontaktuje. Přesto se v poslední době v oblasti podvodných investic do kryptoměn stále častěji objevuje trend, kdy i přes veškeré snahy Komerční banky varovat klienty, že posílají finance na známý podvodný účet, si klienti nedají toto rozmluvit a peníze, často celoživotní úspory, na podvodný účet pošlou, protože mu věří. Narůstá také případů, kdy se e-šmejdi vydávají za bankéři či bankéřku. V tomto případě platí, že si lze jeho či její totožnost ověřit takřka okamžitě ve své bankovní mobilní aplikaci. „Kuriozní jsou i čerstvé případy podvodu, kterému říkáme „*sextortion*“. Začínají se objevovat ve zvýšené míře a podvodníci opravdu neznají mezí, a jsou schopni své oběti vydírat intimními videi a fotografiemi, které jim oběť poskytl, či které fabrikovali pomocí umělé inteligence,“ uzavírá **Marek Macháček**.

Umělá inteligence: nový nebezpečný nástroj v rukách podvodníků

Právě umělá inteligence proniká do kyberpodvodů stále častěji. „Podvodníci dnes umí nejenom napodobit jakékoliv telefonní číslo, ale věrně i hlas volajícího. Oběť tak snadno uvěří, že jí například volá nadřízený, který potřebuje okamžitě proplatit nějakou fakturu. Časté jsou také deepfake videa, kdy e-šmejdi napodobují známé osobnosti a jejich jménem lákají lidi k rádoby výhodným investicím,“ říká **Pavel Šašek**. Zároveň také dodává, že umělá inteligence naopak dobře slouží při odhalování kybernetických podvodů. „Jedná se například o práci s daty, chováním klienta a jeho historií, které se vyhodnocuje v aktuálním čase. Umělá inteligence výrazně automatizuje tyto procesy, zrychluje je a zpřesňuje vyhodnocování,“ doplňuje **Pavel Šašek**.

Jen na vyspělé technologie se spolehnout nelze. Je třeba být obezřetný, používat selský rozum a vzdělávat se

Kybernetické podvody jsou stále sofistikovanější, proto je na prvním místě obezřetnost, zachování klidu a použití zdravého rozumu. „Pokud klientovi volá banka, policie nebo třeba Česká národní banka a chce po něm znát jeho přihlašovací údaje, hesla nebo ho navádí k instalaci jakékoliv aplikace umožňující vzdálený přístup do počítače, je určitě na místě okamžitě zbystřit a telefon raději položit. Vyplatí se i kontaktovat banku a případ nahlásit,“ vysvětluje **Pavel Šašek**. „Důležitá je i edukace. Komerční banka realizuje řadu vzdělávacích kampaní v oblasti kyberbezpečnosti, v loňském roce se například zapojila do kampaně #nePINdej!, jejíž součástí je interaktivní kybertest, díky němuž se zájemci snadno naučí, jak poznat nejčastější kyberpodvody a jak jim nenaletět,“ uzavírá **Pavel Šašek**.

<https://www.kb.cz/cs/o-bance/tiskove-zpravy/efektivita-boje-s-kyberpodvody-roste-komerzni-banka-za-chranila-v-lonskem-roce-klientum-418-milionu>