

Podvodníci míří na účty obcí. Využívají psychologický nátlak i umělou inteligenci

4.8.2026 - Alexandra Kocková | Svaz měst a obcí České republiky

Útočníci stále častěji cílí na zaměstnance a vedení samospráv. Dokážou zmanipulovat člověka s přístupem k bankovnímu účtu obce a připravit ji o statisíce i miliony korun. Ministerstvo vnitra proto obcím předává doporučení Policejního prezidia, jak se před podobnými útoky chránit.

Podvodné útoky už dávno nejsou problémem pouze jednotlivců. Terčem pachatelů se stále častěji stávají také obce, školy, neziskové organizace a další instituce. Podle Policejního prezidia ČR se pachatelé zaměřují na zaměstnance a vedení samospráv, kteří mají přístup k finančním prostředkům. Využívají přitom propracované psychologické techniky, znalost osobních údajů i moderní technologie včetně umělé inteligence.

Ministerstvo vnitra si proto v reakci na dotazy samospráv vyžádalo od Policejního prezidia stanovisko s doporučeními, jak riziko podobných útoků minimalizovat. Svaz měst a obcí ČR nyní tyto informace předává dál, protože právě informovanost a připravenost mohou podle policie významně snížit pravděpodobnost, že útok bude úspěšný.

Falešný bankéř nebo policista může připravit obec o miliony

Jedním z nejrizikovějších způsobů podvodu jsou telefonáty falešných bankéřů a policistů. Pachatel nejprve kontaktuje oběť a tvrdí například, že se někdo pokouší na její jméno sjednat úvěr nebo že je ohrožen její bankovní účet. Následuje psychologický nátlak, který má oběť přimět k rychlému jednání.

Útočníci se vydávají za skutečné policisty, pracovníky bank, České národní banky nebo dalších institucí. Mohou používat jména reálně existujících osob, falešné služební průkazy či dokumenty a vytvářet dojem, že jde o skutečné vyšetřování. Oběť navíc často přesvědčují, že nesmí o telefonátu nikomu říct, případně jí hrozí trestním stíháním či jinými následky.

Situace je o to závažnější, že pachatelé mohou útok cílit přímo na člověka, který má přístup k účtu obce. Mohou ho zmanipulovat k převodu peněz na údajně „bezpečný účet“, k poskytnutí bankovních údajů nebo dokonce k čerpání úvěru.

Podle Policejního prezidia činí u podvodných telefonátů vedených pod legendou falešného bankéře či policisty průměrná škoda více než **700 tisíc korun na jednu oběť**. V některých případech ale škody dosahují **desítek milionů korun**. Jen v letošním roce policie eviduje více než **1 000 registrovaných skutků** s touto legendou.

Terčem nemusí být nezkušený uživatel

Policie zároveň upozorňuje na rozšířený mýtus, že podobným podvodům snadno podlehnou především lidé s nízkou digitální gramotností nebo senioři. Terčem mohou být i velmi vzdělaní a zkušení lidé. U zmíněného typu podvodu je podle policejních statistik typickou obětí žena, a to ve více než 82 procentech případů, průměrně kolem 45 let. Mezi oběťmi jsou například ředitelé a ředitelky škol nebo účetní, které mají přístup k bankovním účtům obcí, institucí či firem.

Pachatelé využívají i umělou inteligenci

Podvodníci navíc své metody neustále zdokonalují. Využívají například technologii **deepfake**. Při videohovoru přes aplikace jako WhatsApp nebo Signal tak mohou dokázat velmi věrohodně zakrýt svou skutečnou identitu. Telefonátu může předcházet také SMS zpráva, která vypadá jako skutečná zpráva banky – například s informací o údajné žádosti o úvěr. Následný telefonát pak působí ještě důvěryhodněji.

Útočníci také využívají takzvaný spoofing, díky kterému mohou podvrhnout telefonní číslo volajícího. Na displeji se proto může zobrazit číslo banky, policie nebo jiného důvěryhodného subjektu. Samotné zobrazené číslo tedy není důkazem, že volá skutečně daná instituce.

Rozhoduje klid a možnost ověření

Základem obrany je podle policie především **přípravenost**. Pokud člověk ví, že se s podobným scénářem může setkat, je mnohem pravděpodobnější, že manipulaci rozpozná. Pachatelé se především snaží vytvořit stres, strach a časový tlak. Oběti nedávají prostor informace ověřovat a přesvědčují ji, aby nikoho dalšího nekontaktovala. Právě tomu je potřeba se vědomě bránit.

Policie a banky své klienty skutečně mohou kontaktovat telefonicky. Nikdy však po nich nepožadují převod peněz na „bezpečný účet“ ani jiné finanční transakce za účelem ochrany finančních prostředků. Pokud je účet skutečně ohrožen, potřebná bezpečnostní opatření přijímá banka sama.

Co dělat při podezřelém telefonátu?

- **Ukončete hovor**, pokud máte podezření, že jde o podvod.
- **Nenechte se zastrašit ani tlačit do rychlého rozhodnutí.**
- Informace si **ověřte přímo u banky, Policie ČR nebo u důvěryhodné osoby** – prostřednictvím kontaktu, který si sami dohledáte.
- Pokud došlo k vyzrazení bankovních údajů nebo podezřelé transakci, **okamžitě kontaktujte banku.**
- **Uchovejte důkazy** a obraťte se na Policii ČR.
- Informujte kolegy a další osoby, které mají přístup k účtům obce. **Pachatelé často těží z toho, že se snaží oběť izolovat.**
- Podezřelé telefonní číslo lze nahlásit operátorovi prostřednictvím SMS na číslo **7726**.

Ochrana obecních peněz je společnou odpovědností

Bezpečnost obecních účtů není pouze otázkou technického zabezpečení. Stejně důležitá je **informovanost lidí, kteří mají k finančním prostředkům obce přístup**. Starostové, zastupitelé, účetní i další zaměstnanci by měli vědět, jak podobný útok vypadá, jaké manipulační techniky pachatelé používají a především že žádná autorita ani časový tlak nejsou důvodem k obejití běžných kontrolních mechanismů. Právě sdílení těchto informací může podle Ministerstva vnitra a Policie ČR významně přispět k tomu, aby se podvodníkům nepodařilo zneužít důvěry lidí a připravit obce o peníze určené jejich občanům.

Svaz měst a obcí ČR proto doporučuje obcím, aby s těmito informacemi seznámily všechny zaměstnance a další osoby, které mohou s obecními finančními prostředky nakládat.

Budte obezřetní. Zastavte se, ověřte si informace a nenechte se dotlačit k rozhodnutí pod tlakem.

Svaz pomáhá obcím připravit se na kybernetické hrozby

Svaz měst a obcí ČR se tématu bezpečnosti a ochrany obecních finančních prostředků věnuje také prakticky. **Ve spolupráci se společností Aliaves jsme proto připravili seminář zaměřený právě na podvodné útoky, jejich rozpoznání a možnosti, jak jim předcházet.** Účastníci se dozvědí, jaké nejčastější scénáře pachatelé používají, na co si dát pozor při telefonické či elektronické komunikaci a jak nastavit v obci účinná preventivní opatření. Cílem je, aby starostové, zastupitelé i zaměstnanci obcí dokázali potenciální útok včas rozpoznat a minimalizovali riziko, že obec přijde o své finanční prostředky.

[Více informací k semináři naleznete zde](#)

Celé znění dopisu Ministerstva vnitra naleznete v přiloženém dokumentu.

Ing. Alexandra Kocková, tiskový zástupce SMO ČR

<https://www.smocr.cz/cs/novinky/a/podvodnici-miri-na-ucty-obci-vyuzivaji-psychologicky-natlak-i-ume-lou-inteligenci>