Ministerstvo
vnitra

MVCRX09AFAKL
prvotní identifikátor

Mgr. Roman Hep
vrchní ředitel sekce veřejné správy

Praha 13. července 2026
Č. j.: MV- 90970-6/ODK-2026

Vážená paní primátorko, vážená paní starostko,

Vážený pane primátore, vážený pane starosto,

v návaznosti na dotazy samospráv ohledně podvodných útoků a vylákání finančních prostředků z obecních bankovních účtů si Odbor veřejné správy, dozoru a kontroly Ministerstva vnitra vyžádal stanovisko Policejního prezidia České republiky. Cílem bylo získat pro obce doporučení, jaká preventivní opatření k ochraně svých rozpočtů přijmout.

Ze stanoviska Policejního prezidia České republiky ze dne 1. července 2026, č. j. PPR-32791-2/ČJ-2026-990340, vyplynulo, že útočníci stále častěji cílí na zaměstnance a vedení samospráv. Zneužívají přitom propracované psychologické techniky a moderní technologie včetně umělé inteligence, jak podrobně vysvětluje Policie České republiky v textu níže.

Tyto policejní poznatky Vám zasíláme k dalšímu využití, zejména k šíření těchto poznatků, jež samo o sobě může výrazně snížit riziko úspěšného útoku v online prostředí na Vaši obec.

V rámci vyžádaného stanoviska Policejní prezidium České republiky upozornilo na následující:

„Kriminalita v online prostředí je na vzestupu, přičemž nejvýraznější nárůst zaznamenáváme v oblasti podvodného jednání. Počet těchto skutků se neustále zvyšuje a pachatelé přicházejí se stále propracovanějšími a důvěryhodněji působícími legendami a způsoby provedení. Často se jedná o cílené útoky, které jsou velmi nebezpečné.

V poslední době zaznamenáváme nárůst případů, kdy oběti nepřicházejí pouze o své soukromé finanční prostředky, ale pachatelé prostřednictvím fyzických osob, které mají přístup k finančním prostředkům firem či institucí, získávají přístup také k účtům zaměstnavatelů. Bohužel se často jedná o finanční prostředky obcí, škol, a neziskových organizací. Nejedná se o zanedbatelné škody. Například u podvodných telefonátů vedených pod legendou „falešný bankéř/policista“ činí průměrná škoda více než 700.000 Kč na jednu oběť. Zaznamenáváme však i případy, kdy škoda dosahuje desítek milionů korun.

Oběťmi těchto podvodů rozhodně nejsou pouze osoby s nízkou digitální gramotností ani primárně senioři, jak se veřejnost někdy mylně domnívá. U zmíněného způsobu podvodu je typickou obětí žena, a to ve více než 82% případů, v průměru ve věku kolem 45 let. Často se jedná o velmi vzdělané osoby, včetně ředitelů a ředitelek škol, kteří bývají častým terčem útoků. Stejně tak evidujeme značné množství případů, kdy se oběti stávají účetní s přístupem k bankovním účtům obcí, institucí nebo soukromých společností.

Ministerstvo vnitra
Nad Štolou 3, 170 34 Praha 7
IČ: 00007064, posta@mv.gov.cz, T: +420 974 811 111
ID DS: 6bnaawp, mv.gov.cz

Nejdůležitější obranou je připravenost na aktuální hrozby. Pokud má potenciální oběť povědomí o současných rizicích a počítá s tím, že se může dostat do obdobné situace, výrazně se zvyšuje pravděpodobnost, že se obětí nestane.

Jako nejrizikovější podvodné jednání současnosti označujeme modus operandi podvodných telefonátů falešných bankéřů a policistů s legendou ohrožení bankovního účtu, při kterém vznikají škody nejen jednotlivcům, ale i obcím a vzdělávacím zařízením.

Podvodné telefonáty falešných bankéřů a policistů

Konkrétní legenda se může mírně lišit, princip však zůstává stejný. Kontaktuje vás osoba vydávající se za policistu nebo pracovníka banky (komerční banky či České národní banky) a snaží se ve vás vyvolat strach tvrzením, že si na vaše jméno někdo chce sjednat úvěr. Útočník využívá kombinaci autority a zastrašování. „Policista“ vás může upozorňovat, že nesmíte nikomu nic sdělit, jinak porušíte mlčenlivost. Pokud odmítnete spolupracovat, může vám vyhrožovat trestním stíháním za legalizaci výnosů z trestné činnosti nebo dokonce údajnou hrozbou vůči vašim blízkým. Pachatelé si oběť mezi sebou často předávají a svá tvrzení podkládají falešnými dokumenty, služebními průkazy či dalšími smyšlenými materiály. Zasílají například i údaje o údajné identitě pachatele, kterého mají vyšetřovat. Oběť nemusí přijít pouze o finanční prostředky na svých bankovních účtech. Pachatelé jsou schopni zmanipulovat ji také k uzavření úvěru nebo ke zpřístupnění finančních prostředků zaměstnavatele.

Manipulace založená na lidském hlasu je velmi účinná a oběť bývá často vystavena intenzivnímu psychologickému nátlaku i několik hodin. Vzhledem k tomu, že se s těším útoky setkáváme již více než pět let, pozorujeme, že pachatelé své argumenty a scénáře neustále zdokonalují. V současné době mají připravené věrohodné odpovědi prakticky na jakýkoliv dotaz.

Zapojení prvků AI - Pachatelé využívají technologii deepfake. V případě, že s vámi komunikují například skrze aplikaci WhatsApp, či Signál, tak se nebrání videohovoru, kdy jsou v rámci videohovoru schopni zastřít svou identitu a video, tak může vypadat velmi věrohodně.

Telefonátu může předcházet také skutečná SMS zpráva zaslaná některou z bank, například s informací o využití telefonního čísla při žádosti o úvěr. Díky tomu může působit celý scénář ještě důvěryhodněji.

Přestože se policii v posledních letech podařilo odhalit a rozbít několik zahraničních call center zapojených do této trestné činnosti, pachatelé ve své činnosti nadále pokračují. Jen za letošní rok jsme zaznamenali více než 1 000 registrovaných skutků s touto legendou.

Manipulace spočívá zejména v následujících technikách:

Využívání síly lidského hlasu

Útočník oběti neposkytuje prostor pro ověřování informací. Jeho postup bývá velmi propracovaný and na většinu dotazů má připravenou pohotovou a věrohodnou odpověď, často v perfektní češtině a s profesionálním vystupováním.

Zneužívání autority
Pachatelé se vydávají za policisty, pracovníky bank, zaměstnance Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) nebo dalších institucí. Často používají jména skutečně existujících osob. Tyto osoby lze následně dohledat na internetu, což může u oběti vyvolat mylný dojem, že tvrzení útočníka jsou důvěryhodná.

Vyvolání strachu
Jde o jeden z hlavních prvků manipulace. Pachatel se snaží oběť uvést do stresu a časové tísně. V takovém stavu lidé často nedokážou situaci správně vyhodnotit and přijímají rozhodnutí, která by za běžných okolností neučinili.

Izolace oběti
Pachatel se snaží zabránit oběti v kontaktu s okolím a přesvědčuje ji, že nesmí nikomu nic sdělit. Často přitom argumentuje smyšlenými sankcemi nebo povinností mlčenlivosti. I proto je důležité poučit všechny členy domácnosti nebo zaměstnance organizace.

Sociální důkaz
Pachatel může například tvrdit: „Tímto způsobem jsme již pomohli mnoha dalším lidem.“ Cílem je utvrdit oběť ve správnosti postupu. V poslední době se navíc setkáváme s konferenčními hovory, během nichž falešný policista a bankéř před obětí sehrávají věrohodně působící rozhovor.

Postupné budování důvěry
Útočníci se často snaží navázat osobnější vztah a hovoří s obětí o běžných tématech, jako je rodina, děti nebo domácí zvířata. Tím si získávají její důvěru a současně prodlužují délku hovoru. Oběť pak nemá prostor kontaktovat někoho dalšího a zároveň jí bývá obtížnější dovolat se z jiného čísla. Evidovali jsme hovory trvající až 12 hodin.

Cílené útoky
Cílený útok na konkrétní osobu bývá výrazně nebezpečnější. Pachatelé znají jméno oběti a často disponují i dalšími, někdy velmi citlivými informacemi získanými například z různých datových úniků.

Cílem pachatele je získat majetkový prospěch. Manipulace proto směřuje zejména k:

- *Předání hotovosti nebo platební karty kurýrovi, který může sdělit předem domluvené fiktivní heslo a předat smyšlené potvrzení o převzetí.*

- *Provedení bankovního převodu na údajně „bezpečný účet“, přičemž pachatelé mohou vytvořit i falešné prostředí internetového bankovnictví.*
- *Vložení hotovosti do zařízení pro nákup virtuálních měn (tzv. bitcoinmatů).*
- *Zneužití technologie NFC prostřednictvím techniky označované jako „červí díra“ (wormhole attack). Pachatel přiměje oběť ke stažení aplikace, která ji vyzve k údajné změně PIN kódu platební karty. Následně oběť navede k přiložení platební karty k telefonu. Současně jiná osoba využije získaná data k výběru hotovosti z bankomatu prostřednictvím dalšího zařízení.*

Je důležité vědět, že policie i banky své klienty skutečně kontaktují telefonicky. Nikdy však nevyžadují provedení finančních transakcí pod záminkou ochrany finančních prostředků. Pokud je účet klienta skutečně ohrožen, přijímá potřebná bezpečnostní opatření sama banka.

Co dělat v případě podezřelého telefonátu:

- *Pokud vás podobným způsobem kontaktuje neznámá osoba a podezřelý telefonát rozpoznáte, hovor ihned ukončete a varujte své okolí. Telefonní číslo můžete nahlásit svému operátorovi prostřednictvím zprávy zaslané na číslo 7726 nebo přidáním hodnocení na specializované webové stránky zaměřené na identifikaci podvodných telefonních čísel.* ***Poznámka****: Útočníci mohou využívat anonymně zakoupené SIM karty nebo technologii tzv. spoofingu CLI, která umožňuje podvrhnout identitu volajícího. Je proto důležité vědět, že vám pachatelé dokáží zobrazit prakticky jakékoliv telefonní číslo. Pokud na takové číslo zavoláte zpět, můžete se dovolat osobě, která s podvodem nemá nic společného.*
- *Nenechte se zastrašit a snažte se zachovat klid. Jakékoliv tvrzení si můžete ověřit, například přímo u dané banky, na Policii České republiky nebo konzultací s osobou, které důvěřujete.*
- *Pokud dojde k vyzrazení citlivých bankovních údajů nebo k provedení podezřelé transakce, neprodleně kontaktujte svou banku.*
- *Nemažte žádné důkazy a obraťte se na nejbližší služebnu Policie České republiky. V případě, že je to možné, tak se pokuste zaznamenat telefonát s pachatelem. Například pomocí diktafonu dalšího telefonu.*
- *Varujte své okolí. Pachatelé se snaží oběť izolovat, proto nestačí poučit pouze jednu osobu v domácnosti nebo organizaci. Informujte své blízké a kolegy.*

Dále doporučujeme sledovat oficiální komunikační kanály Policie České republiky, zejména sociální sítě a webové stránky policie.gov.cz, kde pravidelně zveřejňujeme upozornění na aktuální hrozby.

V rámci modernizace webu Policie České republiky připravujeme také zveřejnění průběžně aktualizovaných informací o současných rizicích v online prostředí, a to nejen v oblasti podvodného jednání, ale také sofistikovaných kybernetických útoků či další kriminality páchané prostřednictvím informačních a komunikačních technologií.“

V případě podrobnějších dotazů se můžete obracet přímo na Policejní prezidium České republiky, úřad služby kriminální policie a vyšetřování.

Pevně věřím, že Vám i lidem ve Vašem okolí tyto informace a doporučení pomohou k zajištění vyšší ochrany (nejenom) veřejných prostředků.

S pozdravem

Mgr. Roman Hep

Adresáti:

všechna města, městysy a obce České republiky

Na vědomí:

1) Svaz měst a obcí České republiky, IČO 63113074, sídlo 5. května 1640/65, Nusle, 140 00 Praha
2) Sdružení místních samospráv České republiky, z. s., IČO 75130165, sídlo Nábřeží 599, Prštné, 760 01 Zlín

Ministerstvo vnitra
Nad Štolou 3, 170 34 Praha 7
IČ: 00007064, posta@mv.gov.cz, T: +420 974 811 111
ID DS: 6bnaawp, mv.gov.cz