Varování před aktuálními telefonními podvody

V současné době čelí většina organizací, orgány veřejné správy nevyjímaje, vlně kybernetických útoků, které jsou prioritně zaměřeny na koncové uživatele. Útočníci stále častěji využívají telefonní podvody označované jako **spoofing**, při kterých se vydávají za pracovníky bank, Policie ČR, České národní banky nebo jiných důvěryhodných institucí.

Proto vám předáváme několik důležitých informací a doporučení.

Vezměte na vědomí, že:

- **NIKDY** vám policista ani pracovník banky nebude volat kvůli „napadenému účtu“ a nepožádá vás o převod peněz na jiný účet.
- **NIKDY** po vás policie ani banka nebudou požadovat výběr hotovosti, převod finančních prostředků ani nákup kryptoměn.
- **NIKDY** vám policie nebude zasílat fotografii služebního průkazu jako důkaz své totožnosti.
- **NIKDY** vás policie nebude přepojovat na pracovníka banky ani banka na policii.
- **NIKDY** po vás banka ani policie nebudou požadovat sdělení přihlašovacích údajů, PINů, autorizačních SMS kódů nebo údajů z platební karty.
- **NIKDY** neinstalujte na pokyn volajícího aplikace pro vzdálený přístup (např. AnyDesk, TeamViewer, Quick Assist apod.)

- Při podezření na nestandardní nebo rizikovou transakci banka zpravidla sama transakci zablokuje nebo ověří její oprávněnost.

Pokud vám volá někdo údajně z banky nebo Policie ČR:

Volající se obvykle představí, uvede své pracoviště a důvod, proč vás kontaktuje. Tyto informace samy o sobě nejsou důkazem jeho totožnosti.

Sdělte mu, že si jeho totožnost a informace ověříte sami. Nikdy neověřujte totožnost prostřednictvím kontaktů, které vám sdělí volající.

Ukončete hovor a ověřte si totožnost volajícího prostřednictvím oficiálních kontaktů:

- u banky zavoláním na oficiální klientskou linku,
- u Policie ČR zavoláním na linku 158.

Pokud vám bude potvrzeno, že vás skutečně kontaktoval zaměstnanec banky nebo policista, požádejte o spojení nebo kontakt na danou osobu prostřednictvím oficiálního komunikačního kanálu.

Pokud si totožnost nemůžete ověřit, nejste si jisti správným postupem nebo máte jakékoliv pochybnosti, hovor ukončete. Oprávněnou záležitost bude možné vyřešit později prostřednictvím oficiálních kontaktů.

- **NIC nepotvrzujte.**
- **NIC nesdělujte.**
- **NIC neinstalujte.**
- **NIKDY neprovádějte převody peněz, výběry hotovosti ani jiné finanční operace na základě pokynů sdělených po telefonu.**

Varovné signály podvodu:

Buďte zvlášť opatrní, pokud:

- volající tvrdí, že vyšetřuje trestnou činnost související s vaším bankovním účtem,
- se na telefonu zobrazí správné číslo banky nebo jiné instituce – číslo může být podvržené (spoofing),
- volající zná vaše osobní údaje (jméno, adresu, číslo účtu apod.),
- vytváří časový tlak („musíte jednat ihned“, „za chvíli bude pozdě“),
- snaží se ve vás vyvolat strach nebo paniku,
- požaduje, abyste zůstali na lince,
- tvrdí, že vás přepojí na policii, banku nebo jinou instituci,
- žádá převod peněz na „bezpečný účet“,
- požaduje instalaci aplikace nebo vzdálený přístup k zařízení.
- během jednoho hovoru nebo navazujících hovorů vystupuje více osob jako policista, bankovní pracovník, pracovník České národní banky nebo bezpečnostní specialista.

Zapamatujte si:

- **NIKDY se nenechte přemluvit.**
- **NIKDY se nenechte přepojit.**
- **NIKDY nikomu nesdělujte své přístupové údaje ani autorizační kódy.**
- **NIKDY neinstalujte software na pokyn neznámé osoby.**

Vždy hovor ukončete a zavolejte zpět sami na oficiální kontakt dané organizace. Pokud si nejste jistí, konzultujte situaci s nějakou nezávislou třetí osobou nebo někým z rodiny.