

### Vishing a spoofing

### Falešné telefonáty

Dnešní technologie jsou už tak daleko, že útočníci dokážou telefonní číslo napodobit. Nenechte se tím ale zmást. Útočník se vydává za pracovníka banky, policistu nebo za zaměstnance ČNB. Snaží se vám namluvit, že jsou vaše peníze v ohrožení nebo máte rozpracovanou žádost o půjčku nebo musíte aktualizovat internetové bankovníctví, protože bylo napadeno. Mohou žádat o výběr hotovosti a vložení do speciálního bankomatu, převod peníze na „bezpečný účet“, dokonce Vám zajistí taxi. Vše pak „stačí“ potvrdit kliknutím na zasláný odkaz. To vás samozřejmě vyděsí.

**Reakce :** Zachovejte klid a pozorně poslouchejte do čeho Vás nutí, rozhodně nesdělujte žádné bezpečnostní údaje, hovor případně okamžitě ukončete. Banka svým klientům neohlášeně nikdy nevolá, na jakékoliv výzvy nereagujte, neklikejte na žádné zasílané odkazy. Banka NIKDY po Vás nebude vyžadovat PIN, přihlašovací údaje nebo posílat odkaz na aktualizaci softwaru.

### Výhodné investování do kryptoměn

Našli jste na internetu reklamu na výhodné investování nejčastěji do akcií nebo kryptoměn, propagovanou známou osobností anebo firmou? Ozval se specialista, který vám chce pomoci s přeposláním vašeho výtěžku z investice, kterou jste provedli? **Dejte si velký pozor!**

**Reakce :** Celebrity jsou využívány jako důvěryhodné osoby, s těmito nabídkami nemají nic společného a sami jsou oběťmi podvodu. Na nabídky prosím nereagujte.

### Bazarové inzeráty

**Ať už zboží prodáváte nebo ho kupujete, buďte obezřetní.** Ozve se vám protistrana a chce s vámi provést platbu za zboží prostřednictvím platební karty nebo např. PayPal. Zpravidla se vám ozve přes WhatsApp nebo mail a pošle vám odkaz, kam vyplníte údaje z karty a přijmete tak peníze. Může chtít také údaje z karty pro kurýra a podobně.

Velmi časně jsou podvody, kdy útočník (zájemce o koupi) nabízí přepravu prostřednictvím kurýra s odkazem na webové stránky, které kopírují reálné weby avšak www adresa není korektní.

**Reakce :** VŽDY si zkontrolujte www adresy, detail e-mailové adresy, kvalitu češtiny, útočník používá falešné, adresa obsahuje podivné znaky. Do bankovních aplikace nepřecházejte ze zasláného odkazu. Neposkytujte údaje ze své platební karty.

### Phishing

Může vám přijít podvodný mail nebo SMS zpráva s odkazem, která se tváří, jako bankovní. Dále chodí zprávy, které lákají na nevyzvednutou zásilku, výhru, žádost o příspěvek na bydlení a spoustu dalších. Odkaz vás ale nakonec navede na „věrnou“ kopii přihlašovací stránky do internetového bankovníctví nebo na přihlášení přes bankovní identitu. Vyradíte tak svoje přihlašovací údaje a pak už stačí jen pár dalších chyb a podvodník se dostane k vašim penězům na účtech.

**Reakce :** Na podobné zprávy nikdy nereagujte, neklikejte na odkazy a nikdy nevyplňujte.

### Falešné odkazy na přihlášení do internetového bankovníctví

Pozor, při vyhledávání webových stránek na internetu můžete narazit na falešné odkazy na přihlášení do internetového bankovníctví. Rovněž můžete narazit na velmi lákavé výhry s odkazy k jejímu vyzvednutí.

**Reakce :** Nenechte se nachytat. Na přihlášení do internetového bankovníctví přistupujte pouze přes webové stránky Banky nikdy ne přes poslané odkazy.

### Romantické dopisy a láska přes internet

„Ahoj, jsem voják v Afghánistánu a potřeboval bych pomoci. Mám tu balíček cenností, které potřebuji dopravit do České republiky. Pomůžeš mi? Stačí jen zaplatit poplatky za dopravu. Slibuji, že hned, jakmile to bude možné, vše ti vrátím a pošlu ještě něco navíc.“

**Reakce :** Na tento druh e-mailu doporučujeme vůbec nereagovat a smazat jej.