

VARUJEME PŘED POSTUPY PODVODNÍKŮ V ONLINE PROSTŘEDÍ

Kyberzločinci neustále mění formu svých útoků, ale principy jejich jednání zůstávají stále stejné. Hrají na **strach, důvěru a časový tlak**, aby přiměli své oběti k ukvapeným rozhodnutím. Vaše **obezřetnost a informovanost** jsou tou nejúčinnější obranou.

Stále se setkáváme s případy, kdy lidé přicházejí o celoživotní úspory jen proto, že uvěřili dobře připraveným legendám a neověřili si pravdivost informací. **Podvodníci, útočí na lidské emoce, zneužívají důvěru a vydávají se za důvěryhodné osoby či instituce.** Je důležité si uvědomit, že **banka, policie ani žádná jiná instituce vás nikdy nebude nutit k nestandardním krokům, převodům peněz či sdělování přístupových údajů.**

NEJČASTĚJŠÍ PODVODNÉ LEGENDY

1. Falešné upozornění z banky

Podvodníci rozesílají SMS nebo e-maily, ve kterých tvrdí, že váš účet je napadený, zablokovaný nebo že proběhla podezřelá transakce. Součástí zprávy bývá **odkaz na falešnou přihlašovací stránku**, kde se snaží vylákat vaše údaje.

Běžné jsou i **telefonáty podvodníků vydávající se za bankovní pracovníky či policisty**, kteří se snaží své oběti přesvědčit, že jejich finance jsou v ohrožení a že je nutné peníze převést na takzvaný „bezpečný účet“. Setkáváme se i s případy, kdy podvodníci přesvědčují oběť k vybrání hotovosti a k osobnímu předání třetí osobě. Banky ani policisté **nikdy** takto nepostupují! Nežádají převod peněz, sdělení autorizačních kódů ani instalaci jakýchkoli aplikací!

2. Investiční podvody

Podvodníci se vydávají za makléře či analytiky a slibují nereálně vysoké zhodnocení peněz. Často využívají sociální sítě, falešné reklamy nebo krypto platformy, které jen napodobují skutečné investiční weby. Pokud vás telefonicky nebo přes mobilní aplikace osloví neznámá osoba, zpozorněte! Nevěřte tomu, za koho se vydává, ani za jakou společnost vystupuje. **Zvažte, reálnost nabízeného zhodnocení!**

3. Falešní technici

Útočníci se představují jako technická podpora počítačových společností, mobilního operátora nebo dokonce banky. Tvrdí, že váš počítač nebo bankovní účet je napaden, a přesvědčují vás k instalaci programů pro vzdálený přístup, které jim umožní převzít kontrolu nad vaším zařízením. Skutečné společnosti vás nikdy nevyzvou k instalaci takových programů.

4. Podvody na sociálních sítích a inzertních portálech

Na tržištích a bazarech podvodníci posílají falešné platební brány nebo se vydávají za kurýrní služby. Snaží se získat údaje z platebních karet nebo přístup k účtům. Dochází také k útokům, kdy podvodníci převezmou váš účet a žádají vaše kontakty o „rychlou finanční výpomoc“.

5. Vyděračské a emocionální podvody

Podvodníci posílají e-maily, ve kterých tvrdí, že mají kompromitující materiály a požadují výkupné. Jindy se vydávají za příbuzného v nouzi nebo za zahraničního „partnera“, který potřebuje pomoc. Příkladem je tzv. **romance scam**, kdy je oběť manipulována k posílání peněz osobě, kterou nikdy neviděla. **Buďte, velmi opatrní při online seznamování. Nikdy neposílejte peníze neznámým lidem, ověřte si identitu a neprozrazujte osobní údaje.**

SKUTEČNÉ PŘÍPADY Z POSLEDNÍ DOBY Z PLZEŇSKÉHO KRAJE

- Senior uvěřil podvodníkovi, který ho přesvědčil, že mu pomůže s neexistujícím „bitcoinovým účtem“. Podvodník získal vzdálený přístup k jeho zařízením a oběť provedla více než dvacet plateb. Celková škoda činila téměř **1 800 000 korun**.
- Žena uvěřila falešnému policistovi a následně falešnému bankovnímu specialistovi. Pod tlakem provedla tři velké převody a vybrala hotovost, kterou předala na parkovišti neznámému muži. Přišla celkem o bezmála **1 600 000 korun**.
- Starší žena se na sociální síti seznámila s údajným námořníkem. Ten ji přesvědčil k odeslání peněz na různé zahraniční účty. Celkově přišla o téměř **1 000 000 korun**.

Tyto případy ukazují, že podvodníci jsou vysoce manipulativní a jejich legendy skutečně fungují – pokud jim dáme příležitost.

JAK SE CHRÁNIT – ZÁKLADNÍ PRAVIDLA

1. Ověřujte si informace

- Pokud vám někdo volá jménem banky, policie nebo instituce, **zavěste a volejte zpět na oficiální číslo**.
- Nikdy nereagujte na nečekané výzvy k převodu peněz.

2. Nesdílejte citlivé údaje

- Hesla, PIN, CVV kódy a autorizační SMS jsou **vaše osobní tajemství**.
- Žádná banka ani policie tyto informace nesbírá.

3. Neklikejte na podezřelé odkazy

- I malá změna v adrese webu může znamenat podvod.
- Pokud si nejste jistí, neotevírejte odkaz.

4. Nepovolujte vzdálený přístup

- Programy typu AnyDesk nebo TeamViewer instalujte pouze na základě vlastního rozhodnutí. Pokud vás někdo nečekaně kontaktuje a požaduje instalaci, ihned to ukončete, jedná se o podvod.

5. Zachovejte klid

- Podvodníci vytvářejí nátlak typu „musíte hned teď“.
- V případě možného podvodu je třeba zachovat klid, vše si ověřit a uvážlivě.

6. Nahlaste podezření

- Pokud máte pochybnosti, obraťte se na svou banku.
- Možný podvod oznamte na čísle **158**.

OSTRAŽITOST SE VYPLATÍ – KYBERZLOČINCI USPĚJÍ JEN TEHDY, KDYŽ JIM DÁTE PŘÍLEŽITOST.

kpt. Bc. Hana Kroftová DiS.

vrchní komisař

+420 974 335 207

+420 602 462 701

hana.kroftova@pcr.cz

KRAJSKÉ ŘEDITELSTVÍ POLICIE PLZEŇSKÉHO KRAJE

Kancelář ředitele krajského ředitelství

Oddělení tisku a prevence

Nádražní 2

306 28 Plzeň

