

VAROVÁNÍ POLICIE ČR

CHRAŇTE SVÉ FINANCE PŘED KYBERPODVOVNÍKY

PODVOVNÍCI OKRÁDAJÍ PŘES SMS!

Neotevírejte bez uvážení
odkazy v SMS, může vás
to stát spoustu peněz.

SMISHING



Krajské ředitelství policie Královéhradeckého kraje



!!! POLICIE VARUJE PŘED KYBERPODVODY !!!

Inzerční reverzní podvody

Nový typ podvodů. Podvedeným bývá člověk, který nabídne bazarové zboží (prodejce) a pachatel (v roli kupujícího) mu zašle odkaz, do kterého požaduje vyplnit údaje k platební kartě.

Častým případem bývá i odkaz s adresou některé přepravní společnosti zajišťující dopravu zboží.

Tipy:

- doporučujeme všímat si formátu webových adres,
- základ webové adresy by měl mít stále stejný kořen: například: <https://www.policie.cz/>,
- všímejte si, aby základní název, v uvedeném případě „policie“, byl stejný a odpovídal obsahu stránky,
- všímejte si koncovek webových adres, aby místo koncovek .cz, .sk, .com, nebyla podezřelá koncovka neznámé země,
- všímejte si drobností, neboť falešné stránky se mohou v drobnostech lišit, například mají navíc tečku, čárku, pomlčku, neaktivní hypertextový odkaz na licenční ujednání dole na webové stránce a jiné,
- jakmile vám přijde způsob provedení prodeje i úhrady neobvyklý, doporučujeme od prodeje raději ustoupit,
- aby vám kupující zaplatili zboží, postačí vždy jen vaše číslo účtu, nikdy není potřeba uvádět údaje k vaší platební kartě.



!!! POLICIE VARUJE PŘED KYBERPODVODY !!!

Falešné webové stránky

Vytvoření falešné internetové stránky dnes zabere i méně nadaným programátorům jen několik řádů minut a takové stránky mohou být téměř k nerozeznání od těch pravých.

Tipy:

- doporučujeme v rámci on-line placení při přesměrování na platební bránu si i kontrolovat stavový řádek webové adresy (kořen adresy by měl být obvyklý),
- doporučujeme nakupovat pouze u obvyklých a osvědčených prodejců, sledovat důvěryhodné recenze,
- zadávejte webové adresy přímo do stavového řádku (kam se píše název webové adresy), nikoli do okénka vyhledávače.

Například u internetového nebo mobilního bankovníctví ideálně v celé nebo zkrácené formě, aniž byste přes zadání slov do vyhledávače, klikali na nabídku placené inzerce. Tato placená inzerce se po zadání hesla do vyhledávače nachází v prvních řádcích výsledků. Tam umísťují své podvržené stránky i podvodníci.

Příklad:

Vezme-li v úvahu již zaniklou agrobanku, budeme-li vycházet z dnešních předpokladů bankovních institucí, tak v případě, že by tato banka dnes ještě existovala a měla webovou adresu, bylo by pravděpodobně možné ji vyhledat po zadání adresy www.agrobanka.cz nebo www.ab.cz.

I JEDNA CHYBA VÁS MŮŽE STÁT VŠECHNY ÚSPORY!

Banky ani Policie ČR po vás NIKDY nepožadují přístupové údaje do internetového bankovníctví, údaje o platební kartě ani PINy!

Přežijte v online světě? Vyzkoušejte si KYBERTEST! www.kybertest.cz



Logo of the Czech Republic Police (Policie ČR) and the National Cyber Security Centre (Národní centrum kybernetické bezpečnosti)



!!! POLICIE VARUJE PŘED KYBERPODVODY !!!

Falešný bankéř/policista

Podvodný bankéř se ozve údajnému poškozenému s informací, že má napadený účet a je zapotřebí, aby okamžitě jednal.

Pozor: Tento pachatel může volat pod maskou telefonního čísla, které se na displeji mobilního telefonu opravdu může zobrazovat jako uvedená bankovní instituce nebo oddělení policie.

Nejčastěji pachatel:

- vyzve poškozeného, že je zapotřebí ochránit finanční prostředky a to tak, že je vloží do bitcoinmatu nebo
- vyzve poškozeného, aby si pro ochranu prostředků nainstaloval program pro vzdálený přístup, který posléze ovládne pachatel. Tím poškozený umožní pachateli, aby skrze zaslané potvrzující sms zaslal peníze na jiné účty.

Tipy:

- důrazně varujeme, bitcoinmat není žádnou úschovnou ani ochranou peněz!
- důrazně varujeme před instalací jakýchkoli programů!
- nikomu cizímu nesdělujte potvrzující sms kódy! Přichází na váš mobilní telefon pouze pro vaši potřebu!
- v případě jakýchkoli pochybností neprovádějte žádná transakce a neprodleně kontaktujte linku 158 a svoji banku.



!!! POLICIE VARUJE PŘED KYBERPODVODY !!!

Falešné nabídky výhodných investic do kryptoměn

Podvodný obchodník se ozve potenciálnímu investorovi s velmi výhodnou nabídkou nebo ho kontaktuje s informací, že z minulého investování má ve virtuální peněžence jistý obnos virtuální měny.

Ale je zapotřebí, aby si jej vyzvedl a to tak, že si má nainstalovat program. Tento pachatel může využít legendu o tom, že program pro vzdálený přístup bude program ke konverzi virtuální měny na běžnou měnu.



Tipy:

- důrazně varujeme před instalací jakýchkoli programů,
- než nějaký program nainstalujete, zjistěte si předem jeho funkce, v případě jakýchkoli pochybností radíme přerušit s nezvaným obchodníkem kontakt,
- v případě jakýchkoli pochybností si ověřujte důvěryhodnost společnosti, např. v obchodním rejstříku nebo i na internetu.



!!! POLICIE VARUJE PŘED KYBERPODVODY !!!

Podvodné seznamovací portály

Podvodníci se vymyšlením různých legend snaží vzbudit v obětech důvěru. A to tak, že si vytvoří falešný profil, stáhnou si fotku z internetu nebo vytvoří fotomontáž a zadají tam falešné údaje.

Často si vybírají lidi staršího věku, osamělé, nemocné nebo handicapované a nabídnou jim pomoc či sblížení, přitom se snaží při dopisování vzbudit soucit a emoce.

Mohou se tvářit jako úspěšní manažeři, právníci, lékaři, sportovci nebo dokonce astronauti. Často slibují, že potřebují částku v řádu tisíců či desetitisíců korun, aby tak mohli poškozenému zaslat více peněz.

Tipy:

- v případě, že jste dotyčného, se kterým se bavíte on-line, do současné doby neviděli, tak si představte, že ten s kým komunikujete, může být někdo úplně jiný, než za koho se vydává,
- důrazně varujeme, abyste pod podobnými záminkami komukoli posílali jakékoli finanční prostředky.

Svým obezřetným a někdy i podezřívavým jednáním můžeme ušetřit sobě nemálo peněz, starostí i času a hlavně internetovým podvodníkům tak nedat šanci!



DEZINFORMACE

SYSTEMATICKÉ A ÚMYSLNÉ ŠÍŘENÍ NEPRAVDIVÉ ČI ZAVÁDĚJÍCÍ INFORMACE

- **PŘÍSTUPUJTE OBEZŘETNĚ KE VŠEM INFORMACÍM Z NEZNÁMÝCH A NEOVĚŘENÝCH ZDROJŮ.**
- **NESDÍLEJTE NEOVĚŘENÉ INFORMACE - ČÍM SENZAČNĚJŠÍ INFORMACE, TÍM VÍCE JE DŮLEŽITÉ OVĚŘIT SI JEJÍ PŮVOD.**
- **INFORMACE OVĚŘUJTE DOHLEDÁNÍM DŮVĚRYHODNÉHO ZDROJE, IDEÁLNĚ V POROVNÁNÍ S VÍCE RŮZNÝMI A DŮVĚRYHODNÝMI MÉDII.**
- **PŘÍSPĚVKY S NEDŮVĚRYHODNÝM ZDROJEM MŮŽETE NAHLÁSIT SPRÁVCI SOCIÁLNÍ SÍTĚ - TAKOVÝ OBSAH JE NYNÍ S VĚTŠÍ DŮSLEDNOSTÍ ODSTRAŇOVÁN.**
- **NEREAGUJTE NA DEZINFORMACE, ANI KDYBYSTE JEN CHTĚLI UPOZORNIT NA JEJICH NEPRAVDIVOST (tzv. debunking) - ZVÝŠIL BY SE TAK DOSAH ZPRÁVY.**

DEZINFORMACE JSOU CÍLENĚ ŠÍŘENY DLOUHODOBĚ I ZCELA BEZPROSTŘEDNĚ V REAKCI NA AKTUÁLNÍ DĚNÍ, A TO ZEJMÉNA NA SOCIÁLNÍCH SÍTÍCH (Facebook, Instagram, Twitter - X, Telegram, YouTube atd.), ALE I PROSTŘEDNICTVÍM TZV. DEZINFORMAČNÍCH WEBŮ. TAK JE CÍLENĚ PODRÝVÁNA VĚROHODNOST BĚŽNÝCH SDĚLOVACÍCH PROSTŘEDKŮ A OFICIÁLNÍCH ZDROJŮ INFORMACÍ.

POMOCÍ LŽÍ, POLOPRAVD, RELATIVIZACE FAKTŮ A MANIPULACE TATO STRATEGIE PROVOKUJE SPOLEČNOST K PODPOŘE NEDEMOKRATICKÝCH A EXTRÉMISTICKÝCH POSTOJŮ, VŠTĚPUJE JÍ POCIT BEZMOCI V RÁMCI DEMOKRATICKÉHO SYSTÉMU A OBECNĚ PODKOPÁVÁ DŮVĚRU VE STÁT A JEHO INSTITUCE.

- **NENÍ VHODNÉ SDÍLET PŘÍSPĚVKY Z NEOVĚŘENÝCH ZDROJŮ, TÍM BY SE POUZE ZVÝŠIL DOSAH FALEŠNÉ INFORMACE.**
- **OVĚŘENÝMI ZDROJI INFORMACÍ JSOU VEŘEJNOPRÁVNÍ MÉDIA A OFICIÁLNÍ WEBOVÉ STRÁNKY STÁTNÍCH INSTITUCÍ.**

