

[Úvodní strana](#) / [Informační servis](#) / [Zpravodajství](#)

Zpravodajství

## Důvěřuj, ale prověřuj! Před Vánocemi dvojnásob...

Internetoví podvodníci se před koncem roku opět snaží nachytat neopatrné uživatele internetového prostředí. Sice nevymysleli nic nového a užívají staré triky, ale jak je vidět, jsou to triky osvědčené a bohužel stále fungující.

Obzvláště v této uspěchané době, kdy se vlivem událostí přesunulo velké množství běžných činností do virtuálního světa Internetu, buďte opatrní a veškeré úkony číňte s rozvahou a po důkladném rozmyslu. Důvěru je třeba si hýčkat a ne s ní zacházet jako s reklamním letákem!

Policisty v současné době zaměstnává zvýšený počet poškozených, kteří se díky své důvěřivosti a neopatrnosti stali obětí podvodu. Zejména se jedná o podvod s nabídkou společného života doplněnou žádostí o finanční pomoc a dále snahy vylákat od uživatelů internetového bankovníctví přístupové údaje k jejich bankovním účtům a platebním kartám.

### "AMERICKÝ VOJÁK"

V prvním případě má scénář podvodu různé podoby, které ale spojují společné prvky. Interně se tento podvod nazývá podle původního případu falešné identity „Americký voják“. Je postaven na modelu získání důvěry zejména osoby opačného pohlaví pod záminkou společné budoucnosti. Ústřední postavou tohoto podvodu a tedy vymyšleného příběhu bývá cizinec, který se snaží zkontaktovat osobu (oběť) přes různé komunikační portály, ať už seznamky či sociální sítě a vždy se zašití příběhem. V tomto příběhu jde o zlato, peníze či jiné cennosti, případně o jeho život. Vždy je třeba mu pomoci dostat tyto komodity z nějakého nebezpečného místa. Nejčastěji jsou to místa typu Afghánistán, Sýrie a další státy s nestabilním režimem a přítomností mezinárodních sil.

Tento podvodník se zpravidla vydává za amerického vojáka, námořníka, právníka, lékaře či úředníka, ale i umělce, kteří jsou zde na misi nebo mají možnost získat třeba dědictví a potřebují nalézt někoho, kdo jim pomůže s vyvedením zmiňovaného bohatství mimo nebezpečnou zemi, případně jim pomůže se záchranou života. Následuje samozřejmě příslib společné budoucnosti se zajištěným člověkem, popřípadě příslib na podíl z majetku. Objevil se i příběh námořníka bojujícího o život na potápějící se lodi. Dalším společným momentem jsou opakující se žádosti o zaslání finančních prostředků na zařízení potřebných postupů k převedení finanční hotovosti, vyvezení zlata ze země či vyřízení výjezdních povolení a úplatků pro místní autority. Komunikace probíhá přes chaty a emaily. Mnohdy za využití Google překladače.

Myslíte si, že na takovéto „pohádky“ nemůže nikdo naletět? Omyl... Osamělí lidé a např. lidé v těžké životní situaci hledají někoho, kdo jim dá nový cíl a impuls. A tím může být i záchrana života člověka či příslib nového vztahu. Policisté bohužel evidují případy, kdy oběti podvodníků, nejčastěji ženy, zaslaly finanční prostředky v rozmezí tisícových až milionových částek.

Komunikujete s někým, jehož příběh se podobá výše popsanému nebo znáte někoho, kdo tento příběh prožívá? Budte opatrní a nikomu neposílejte žádné finanční prostředky. O tom samém zkuste přesvědčit svou známou. Vždy v takovýchto případech poproste o názor dalšího člověka, který se na vše bude dívat nezatížený předešlou romantickou či naléhavou komunikací.

### VYLÁKÁNÍ PŘÍSTUPOVÝCH ÚDAJŮ K PLATEBNÍM KARTÁM A INTERNETOVÉMU BANKOVNICTVÍ

Druhou formou podvodů dnešní doby je snaha pachatelů o získání přístupových informací k vašemu internetovému bankovníctví a využitelných údajů vaší platební karty. Přišel vám do té vsí předvánoční záplava emailů a sms zpráv požadavek na aktivaci vašeho bankovního účtu či aplikace v telefonu? Je po vás najednou vyžadováno využití aktivizačního klíče? Objevila se zde zpráva o zablokování vašeho účtu? Přišla vám výzva k zadání údajů z platební karty k jejímu odblokování či autorizaci?

#### Čeho se vyvarovat?

Byl vznesen požadavek na doplatek za dopravu vámi objednaného zboží? Jste právě krok od toho stát se obětí podvodníka!

V případě, že

- budete reagovat na pokyny ve zprávách a poskytnete soukromé soukromé informace;
- se necháte odkazem přeměrovat na stránky, které jsou k nerozeznání od stránek vaší banky;
- komunikativně sdělíte kód (bezpečnostní, ověřovací, jednorázový), který vám přišel nečekaně;
- zkrátka uvěříte, že banky takto komunikují se svými klienty;

dáte podvodníkům jedinečnou šanci bezpracného výdělků na váš účet.

#### Jak se bránit?

- Na takovéto zprávy a výzvy nereagujte;
- nikdy se nenechávejte přeměrovat na stránky vašeho internetového bankovníctví přes odkazy ve zprávách;
- vždy využijte zadání přímé cesty do internetového bankovníctví tak, jak jste zvyklí;
- v případě pochybností kontaktujete telefonickou linku vaší banky a ověřte si jejich požadavek;
- věřte tomu, když policie a všechny bankovní instituce říkají: „Banky po klientech nikdy nepožadují zadávat citlivé informace formou emailových či sms zpráv“.

Opět evidujeme mnoho případů, kdy z neopatrnosti došlo ze strany poškozených k předání autorizačních údajů podvodníkům. Následně tito ovládli internetové bankovníctví účtu klienta a vyvedli z nich finanční prostředky. Říkáte si, že to není váš případ? Že se Vám to stát nemůže, jelikož na účtu nemáte finanční prostředky? I v takovém případě ale může dojít k nemalé škodě na vašem majetku. Podvodníci si po ovládnutí účtu poškozeného dokáží vyřídit online půjčku a do několika hodin být bohatší třeba o 50.000,-Kč.

Máte podezření a nevíte co s tím? Vždy je lepší se poradit než poté naříkat. Nic není tak naléhavé, aby to nemohlo počkat na ověření, třeba do následujícího dne.

Budte proto obezřetní a ověřujte si informace. Jde o VAŠE peníze...

18. 12. 2020

Důvěřuj, ale prověřuj! Před Vánocemi dvojnásob... - Policie České republiky

kpt. Bc. Ondřej Penc  
oddělení prevence  
11. 12. 2020

© 2020 Policie ČR, všechna práva vyhrazena