

Nenaletěte podvodníkům, internetové podvody jsou stále sofistikovanější

Policie České republiky, Obvodní oddělení Ústí nad Orlicí, si Vás dovoluje stručně seznámit s nejčastěji se vyskytujícími internetovými podvody, které za poslední dobu policie zaznamenává nejen při příjmu oznámení od poškozených občanů na zdejší služebně, ale rovněž se vyskytujících po celé ČR. Podvodníkům se dobře daří obelstít ty méně zdatné a méně informované uživatele internetu, ale také ty příliš důvěřivé či zvědavé.

Dnešní doba nám umožňuje přes různé internetové servery uskutečnit velkou část pracovních povinností, získávat různé informace, zprostředkovávat nákup či prodej zboží nebo se zkontaktovat s přáteli či rodinou. Podvodníci z Vás pod různými přísliby vydáváním se za přátele, za firmu nebo spolehlivé kupující, nabízením investic, falešně se vydávající za policisty, bankéře, ropné magnáty, vojáky a tak dále, vylákají nemalé finanční částky.

Problémem obecně je, že pachateli nabyté finanční částky míří na zahraniční bankovní účty nebo do tzv. kryptoměn (virtuální měny), kde je koncový příjemce velmi obtížně, ne-li někdy vůbec, dohledatelný. Částečným klíčem k řešení vzniklého problému je rychlost konání po zjištěném podvodu, protože stopy v kyberprostoru rychle mizí. Vaše první kroky by proto měli vést do banky (příp. přes telefonickou podporu banky), někdy je totiž možné již uskutečněnou platbu stornovat.

Bohužel do krátkého článku není možné podrobně popsat podvod od podvodu, zahrnout zde základy fungování na internetu, ani Vás srozumět se všemi nástrahami v internetovém prostředí. Níže Vás alespoň seznámíme s těmi nejčastějšími triky těchto podvodníků.

1) „Podvodník s PINem“ - Váš údajný přítel (např. na Facebooku či Instagramu) chce od Vás získat PIN (heslo, kód), který Vám nechá zaslat na Vaše telefonní číslo

V rámci sociálních sítí Vám přijde zpráva od přítele s tím, že o něco soutěží a rychle potřebuje Vaše telefonní číslo. Následně žádá zaslat PIN, který Vám přijde do SMS zprávy. **Lámanou češtinou** Vás ujišťuje, že nemůže nastat žádný problém. Je podezřelý, že se zprávy s pokyny o zaslání PINu neustále opakují, přítel s Vámi ve skutečnosti nekomunikuje. Tento účet Vašeho přítele může být napaden, někdo mohl uhodnout heslo k jeho účtu, a teď se za něj vydává. Také někdo mohl napodobit jméno Vašeho přítele a založit účet nový. **Pokud podlehnete a PIN zašlete, bude Vám stržena platba za telefonní tarif, a na konci měsíce budete žasnout nad fakturou.**

Rada zní – **skryjte před ostatními seznam svých přátel** na Facebooku, Instagramu, příp. na dalších sociálních sítích, podvodník tak nebude mít komu napsat. **Pokud vám přijde SMS s jednorázovým heslem na potvrzení transakce přes m-platbu, kterou jste si neobjednali, rozhodně heslo nikomu nesdělujte!** Zdá-li se Vám konverzace od Vašeho přítele na sociálních sítích podezřelá, zkuste si to raději ověřit jiným způsobem – např. kamarádovi zavolejte, zeptejte se ho osobně. **Zabezpečte si své účty dostatečně bezpečným heslem, ideálně kombinací velkých a malých písmen či čísel. Ideálně svá hesla pro přihlášení nikde neukládejte, nezůstávejte nikde přihlášení (zejm. na jiných zařízeních, než jsou ta Vaše).**

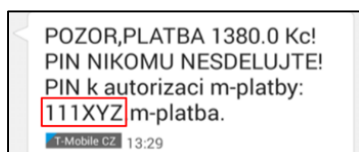
Dva příklady, jak mohou vypadat přijaté zprávy (konverzace) na Facebooku, kterou Vám podvodník zašle:



Obrázek 1 - Pachatel chce „naléhavě“ Vaše tel. číslo, uvádí, že soutěží, opakovaně žádá heslo (PIN)

Dva příklady, jak může vypadat SMS zpráva pro potvrzení m-platby:

Obrázek 2 - Ukázka SMS zprávy s PIN kódem pro potvrzení m-platby



Obrázek 3 – Jiná ukázka potvrzení m-platby v SMS zprávě s PIN kódem



2) „Podvodník bankéř“ - Volá Vám údajný pracovník Vaší banky s informací, že máte napadený bankovní účet, druhý telefonát může být od údajného policisty

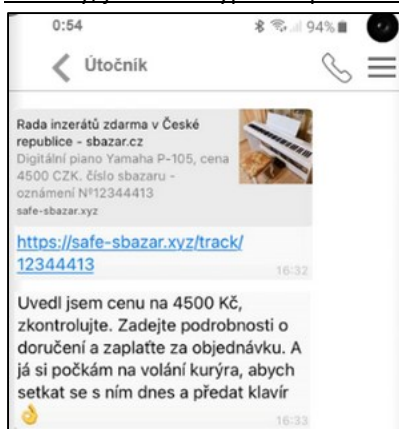
Tento bankéř Vám doporučuje, že si máte okamžitě peníze převést na jiný účet, nebo je vybrat a např. vložit do kryptoměny, elektronicky nebo pomocí „bitcoinmatu“ (to je přístroj podobný bankomatu, vložíte do něj hotovost a tyto peníze se „přemění“ na virtuální měnu). Dále Vás může tlačít do nainstalování jakési aplikace do telefonu či počítače (např. „AnyDesk“). Po tomto telefonátu může následovat ještě telefonát od údajného policisty, který napadení Vašeho účtu potvrdí.

Opravdu pozor. Tito podvodníci mají hned několik různých historek a následných řešení. Cíl je však vždy stejný - **snaží se ve Vás vyvolat strach** o finance, **vytváří na Vás tlak** tím, že se všechno musí udělat ihned, jinak o peníze přijdete. **Stejným způsobem Vás mohou tláčit do investic** např. do zlata, různých fondů nebo opět kryptoměn. **Bohužel umí napodobit telefonní čísla bankovních institucí i policie!** **Pracovníci banky (ani příslušníci policie) po Vás NIKDY SAMI OD SEBE nebudou chtít údaje k bankovnímu účtu či kartě telefonicky, po SMS nebo e-mailem.** Máte-li o své finance strach, běžte si skutečnost raději **ověřit osobně** na pobočku banky, příp. kontaktujte banku telefonicky na jejich asistenčních službách.

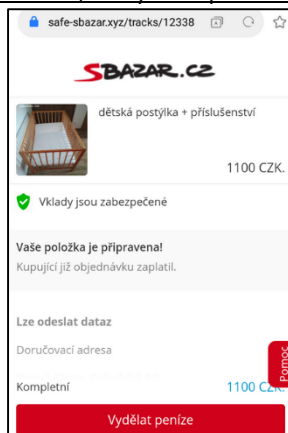
3) Podvodník „Nákupčí“ - Pokud něco prodáváte, nikomu neposílejte, ani nikde nezadávejte své bankovní údaje! Kupujícímu k zaslání peněz stačí číslo bankovního účtu.

Podvodníci na Vás při nákupu Vámi inzerovaného zboží zkouší, že si toto zboží převezmou přes nějakou dopravní společnost či kurýra. Nebo mohou poslat odkaz se „zabezpečenou“ platbou, kdy na zasláném odkazu si máte vyzvednout peníze, které tam údajně již poslal. Odkazy, které zašlou, Vás později donutí zadat údaje k Vaší platební kartě. **Vy prodáváte, nemáte tedy důvod kamkoli zadávat údaje k Vaší platební kartě! Kupující víc než Vaše číslo bankovního účtu nepotřebuje. Nenechte se napálit!** Podezření by ve Vás měla vyvolat zejm. lámaná čeština, dále podvodníci odmítají přebírku zboží jiným způsobem (tzn. ani osobně, přes Zásilkovnu, Českou poštu,...).

Příklady, jak může vypadat zpráva od podvodníka, který Vám posílá odkaz na kurýrní službu nebo jakousi

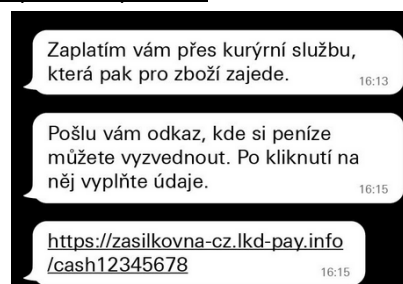


Obrázek 5 - Pachatel Vám zasílá podezřelý odkaz, v textu je patrná lámaná čeština



Obrázek 5 – Po kliknutí na odkaz se zobrazí toto. Po kliknutí na „Vydělat peníze“ začne stránka vyžadovat údaje z Vaší platební karty

„zabezpečenou platbu“:



Obrázek 4 - Pachatel zasílá podezřelý odkaz k vyzvednutí peněz

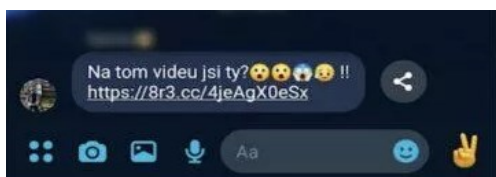
4) Dávejte pozor na podezřelé odkazy v konverzacích na sociálních sítích nebo v e-mailu

Podvodníci se vydávají např. za Českou poštu a další doručovací společnosti, za různé bankovní instituce, obchodníky. Prozradit je může špatný pravopis, rozdílná e-mailová adresa od skutečné, lámaná čeština. Nejste si jisti? Telefonicky si informace ověřte u daných institucí! Řiďte se zdravým rozumem. **Neklikejte hned na každý odkaz, který Vám přijde! Podezřelé informace si ověřujte jinými možnými způsoby. Mějte své účty důsledně zabezpečené, zvolte špatně uhadnutelná hesla, ideálně různá hesla na různé účty. Používejte ověřené antivirové programy.**

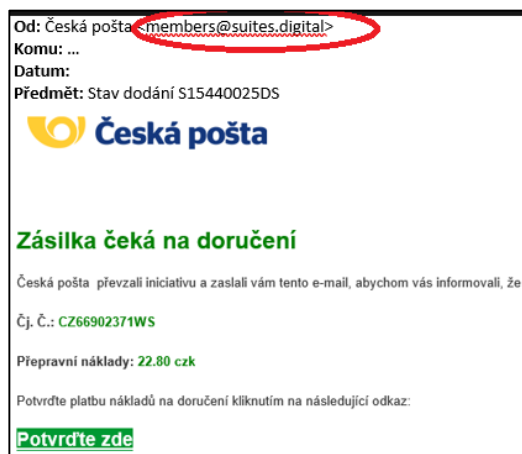
Obrázek 7 - Ukázka podvodné SMS, která Vám může přijít na mobil



Obrázek 8 - Ukázka podvodné zprávy na Facebooku, příchozí adresa je podezřelá kombinací písmen a čísel. Zde podvodník využívá Vaši zvědavost, kliknutím na odkaz a zadáním svých údajů, např. k přihlášení na Facebook, můžou pachatelé získat Vaše citlivé údaje



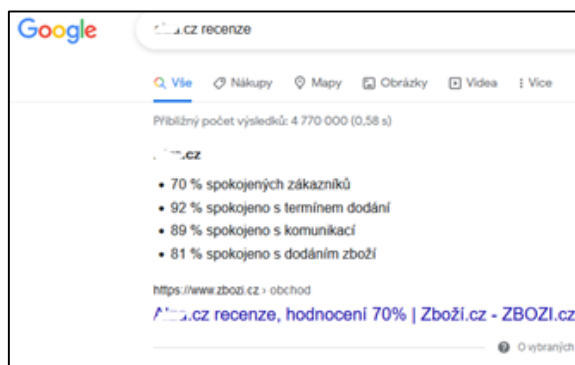
Obrázek 6 - Ukázka podvodného e-mailu, kde se pachatelé vydávají za Českou poštu,



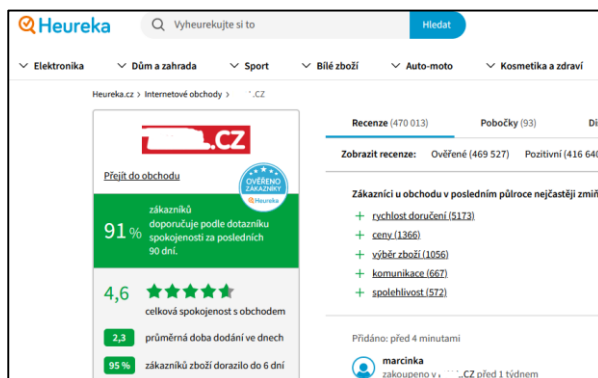
5) Ověřujte si kvalitu internetového obchodu, ze kterého objednáváte zboží

Jde to úplně jednoduše, např. tak, že zadáte do internetového vyhledávače adresu tohoto obchodu spolu se slovem „recenze“. Dalším spolehlivým ukazatelem kvality obchodu je vyhledávač „Heureka.cz“.

Obrázek 9 - Použijte ověřený vyhledávač (např. google.com, seznam.cz), pro ověření recenzí obchodu



Obrázek 10 - Např. „heureka.cz“ je ověřený srovnávač cen a recenzí obchodů



6) „Podvodník Zamilovaný voják (aj.)“ - Pozor při randění na seznamovacích serverech

Zdroj: policie.cz, root.cz, jaknainternet.cz, peníze.cz, podvodnici.eu, ceskaposta.cz, zasilkovna.cz, blog.avast.com, gopay.com/blog, pribram.cz (Tomáš Pečenka, autor čl. o podvodech na internetu)

Abyste se nestali obětí seznamovacího podvodu, dodržujte následující rady:

- dobře zvažte, zdali přijmete nabízené přátelství od neznámého člověka na internetu
- dávejte si pozor na sliby týkající se vážného vztahu, zejména s osobou ze zahraničí
- protistrana dokáže velmi citlivě působit zejména na osamělé osoby, milá slova, lichotky
- bývají rozvedení nebo vdovci a touží po vážném a harmonickém vztahu
- předstírají intenzivní zájem o vaše soukromí, vědí, co osamělá žena potřebuje
- své oběti zpracovávají sladkými slůvky několik týdnů i měsíců
- **po určité době přichází se svými požadavky a to formou finanční pomoci** např. na proclení cenného balíčku, na lékařské ošetření, pomoc po okradení, investice do podnikání....
- **nesdílejte s nikým vaše intimní fotografie**, mohou být později zneužity k vydírání

Shrnutí rad, jak se nestát podvedeným:

- ***Pokud vám přijde SMS s jednorázovým heslem na potvrzení transakce přes m-platbu, kterou jste si neobjednali, rozhodně heslo nikomu nesdělujte!***
- ***Zdá-li se Vám konverzace od Vašeho přítele na sociálních sítích podezřelá, zkuste si ji raději ověřit jiným způsobem (telefonicky, osobně)***
- ***Zabezpečte si své účty dostatečně složitým heslem, ideálně kombinací čísel, velkých a malých písmen, nedávejte si na všechny účty stejné heslo, neukládejte si hesla na cizí zařízení***
- ***Nevěřte všem e-mailům a neklikejte na všechny odkazy, které Vám do Vašich e-mailových schránek nebo do zpráv na sociálních sítích dorazí***
- ***Pozor na neznámé volající, kteří se představují jako bankovní úředníci, specialisté k investování***
- ***Nesjednávajte si žádné půjčky ani investice telefonicky, neinstalujte si neznámé aplikace do svých zařízení na žádost cizích osob***
- ***Nikomu na jeho žádost nefoťte svou platební kartu z obou stran, dávejte pozor, kam tyto údaje zadáváte (buďte obezřetní při nákupu a zejm. prodeji!)***
- ***Nejste-li si jistí, ptejte se! Svých dětí, vnuků, rodičů, bankovních ústavů či policie. Raději se dvakrát zeptat, než jednou litovat...***
- ***Jestliže jste se stali obětí podvodu, jednejte co nejrychleji, zejm. oslovte svou banku ohledně učiněné platební transakce, s podvodníky již dále nekomunikujte, na příp. výhružky nereagujte***
- ***Opravdu si rozmyslete, s kým v „elektronickém světě“ komunikujete, protože některé věci, jako např. zaslání Vašich intimních fotografií, zpět už nevrátíte***

Co se týče výše uvedených podvodů, jedná se pouze o jejich krátký výčet a o stručné seznámení s nimi. Po zadání slovního spojení „internetové podvody“ do internetového vyhledávače, získáte spoustu dalších informací a také více ukázek, jak takové podvody vypadají. Dávejte pozor na sebe, své blízké a také na své finance.

Policie ČR, Obvodní oddělení Ústí nad Orlicí