

POČET ONLINE PODVODŮ EXTRÉMNĚ NARŮSTÁ, UŽIVATELÉ DĚLAJÍ STÁLE STEJNÉ CHYBY

Kamil KOPECKÝ

Počet podvodů páchaných v online prostředí v posledním roce razantně narostl, kromě běžných dobře známých podvodů se objevily nové formy podvodného chování, které začaly aktivně cílit například na uživatele, které v online prostředí prodávají zboží. Narostl také počet podvodů spojených s investicemi do kryptoměn, které slibují rychlé zbohatnutí. Stále populárnější se stává také vishing, tedy druh podvodného telefonátu.

Cíl podvodníků pak zůstal stejný - **vylákat z uživatelů citlivé údaje, ovládnout jejich bankovní účty a převést z nich co nejvíce finančních prostředků**. Základním motivem pachatelů je tedy **zisk**.

V posledních letech vzrostl počet podvodů především na [inzerčních portálech](#) - podvodníci se totiž začali zaměřovat na prodejce zboží a prostřednictvím podvodné stránky z nich vylákávají přístupové údaje k platební kartě či účtu.

Na podvody však narazíme i při běžném prohlížení internetu - třeba na zpravodajských portálech či sociálních sítích. Ty totiž na svých stránkách nabízejí reklamní prostor externím společnostem a hrozí reálné riziko, že se zde objeví podvodná reklama. V prostředí sociálních sítí také narazíme na hacknuté účty, které velmi často podvodné zprávy šíří mezi další uživatele.

Hoaxy, které vypadají jako předvolání od policie

Velmi populární jsou také podvodné zprávy, které **vypadají jako předvolání k soudu** za to, že jste ze svého počítače sledovali zakázaný pornografický obsah. Můžete však zaplatit pokutu a tím se obvinění zbavíte! Samozřejmě jde o podvod - cílem podvodníků je vystrašit nás a přimět k ukvapené reakci, tedy platbě, ve skutečnosti však policii či soudu nic neplatíme, ale sponzorujeme podvodníka.



Ukázka podvodného předvolání

Variant tohoto podvodu je mnoho, k populárním verzím např. patří, že nás policie (či někdo jiný) sledovala při masturbaci před nelegálním obsahem, a abychom se vyhnuli obvinění a zveřejnění materiálů, musíme uhradit pokutu. Ostatně vyděračský e-mail si můžete vyzkoušet pomocí našeho simulátoru zde: <https://e-bezpeci.cz/fakeemail/>.

Podvody s kryptoměnami

Jak již bylo řečeno, k poměrně novým typům podvodů patří také **podvody spojené s investicemi a kryptoměnami**. Na úvod je třeba říci, že mnoho z těchto podvodů využívá “falešnou reklamu s celebrity”, které doporučují tuto investici jako skvělý způsob zbohatnutí, o kterém samozřejmě média mlčí. Reklama pak vede na stránky, kde můžeme projevit zájem o zaručeně výdělečnou investici, pokud zde zanecháme své telefonní číslo. Jakmile to uděláme, ozve se nám (např. telefonicky) “pracovník”, který nám vysvětlí, že je třeba nainstalovat do našeho počítače program pro přístup ke vzdálené ploše, pomocí kterého bude přes náš účet daná instituce investovat (u některých typů podvodu investují “živí lidé”, u jiného různí automatictí roboti) a zajistí nám trvalý zisk. V řadě případů oběti dobrovolně transakce autorizují např. přes SMS, protože si myslí, že jde o onu slibovanou výnosnou investici, např. nákup bitcoinů či jiné kryptoměny. Ve skutečnosti však přicházejí o své finance. Tento podvod existuje v mnoha různých variantách,

takže pozor na jakoukoli instalaci neznámého software do našeho počítače či mobilního telefonu.

Vishing

Jak jsme si demonstrovali výše, mnoho podvodů současnosti využívá tzv. **vishing**, ve kterém se pachatelé vydávají např. za bankéře či policisty, kteří se snaží pomocí telefonického hovoru vystrašit klienty různých bank legendou o napadení jejich účtu a nutností učinit další bezpečnostní kroky pro záchranu svých financí. Tito podvodníci působí skutečně věrohodně a v řadě případů dokázali přimět klienty k tomu, aby si do svých počítačů nainstalovali program pro vzdálený pořístup, přes který poté pachatel pronikl do bankovního účtu a převedl z něj finance. Z těchto účtů jsou pak zpravidla finanční prostředky velmi rychle vybrány a do několika hodin po převodu účty zmizí.

Staré dobré legendy stále táhnou - romance scam, CEO scam a invoice scam

Stálicemi na poli online podvodů jsou zcela jistě romance scam, CEO scam a invoice scam.

Romance scam je podvod, který využívá především osamělosti. Pachatelé předstírají, že mají zájem o navázání romantického vztahu právě s vámi - jsou osamělí, bohatí, ale dosud nenašli svůj vhodný protějšek (např. z časových či jiných důvodů). Předstírají, že jsou např. američtí vojáci vracující se z misí v zahraničí, kteří jsou finančně zabezpečeni a kteří se chtějí usadit v ČR, lékaři pracující v zahraničí, inženýři, osamělí manažeři či dokonce bohatí princové stěhující se do Evropy apod. Jakmile získají důvěru oběti, začnou žádat o finanční pomoc - např. potřebují poskytnout menší peněžní půjčky např. na cestovné, celní poplatky, bankovní poplatky apod. Romance scam obvykle míří na osamělé starší osoby (velmi často v důchodovém věku), a to jak na muže, tak i na ženy. Existuje však také varianta romance scamu zaměřená na muže středního věku. Mladá a krásná žena (obvykle z ukrajiny či ruska) se touží provdat do ekonomicky zajímavější země a hledá

hodného, staršího (a také solventního) muže. Scénář se opět opakuje - po počáteční fázi kontaktu začne pachatel po vyhlédnutém muži chtít z nejrůznějších důvodů finance.

Dalším druhem scamu, který je rozšířený především ve firmách, je tzv. **boss scam** či **CEO scam**. V tomto případě podvodník pomocí e-mailu předstírá, že je náš nadřízený (např. ředitel, vedoucí pracovník), který požaduje okamžitý převod finančních prostředků z firemního účtu na jiný účet (např. uhrazení fiktivní faktury, pokuty, poplatku apod.). Pachatelé umí změnit jméno, příjmení a e-mailovou adresu uvedenou v e-mailu, takže je e-mail na první pohled uvěřitelný. Tento typ podvodu cílí především na větší firmy, které zpracovávají velké množství faktur.

Řada firem (a také škol) má zkušenost také s tzv. **invoice scam** či podvodnými fakturami. Jde o velmi rozšířený druh scamu ve formě e-mailů s fakturami za neobjednané zboží či služby (třeba registrace do různých katalogů, nedoplatky, dlužné částky), které bohužel mnoho institucí automaticky proplatí. Hrozba sankcí za nezaplacení faktury je navíc silná motivace pro to, abychom přiloženou přílohu otevřeli, čímž můžeme svůj počítač, případně celou školní či firemní síť vystavit riziku počítačového viru. Mnoho z těchto příloh totiž obsahuje také počítačový malware (virus). K nejnebezpečnějším virovým hrozbám pak patří zejména tzv. ransomware, který pronikne do počítače, zašifruje vaše soubory a za jejich odemknutí požaduje finance.

Další informace o online podvodech nalezneš v našem videoseriálu [Prevíti na síti](#).

Doporučení

Internet nám nabízí velké množství pozitiv. Při jeho využívání však nesmíme zapomínat na dodržování bezpečnostních zásad, ke kterým patří zejména tyto:

1. **Používat antivirový program, který zajistí, aby se do našeho počítače nedostal nežádoucí malware.**
2. **Pravidelně aktualizovat operační systém a jednotlivé**

-
- programy, zálohovat si důležitá data.**
- 3. Používat legální software.**
 - 4. Nikdy neposkytovat své osobní a další citlivé údaje osobám, které známe pouze z internetu. V žádném případě nikomu neposkytovat své vlastní intimní materiály - fotografie a videa.**
 - 5. Neotvírat přílohy e-mailů z neznámých zdrojů!**
 - 6. Nenechat se nachytat na e-maily, které slibují rychlé zbohatnutí, navázání romantického vztahu či výhry v loterii. Jde s vysokou pravděpodobností o podvody.**
 - 7. Ověřovat si veškeré důležité informace - např. zatelefonovat do banky, zatelefonovat svému vedoucímu, poradit se s experty.**
 - 8. Pokud se staneme obětí podvodu, nebát se kontaktovat Policii ČR!**
 - 9. V případě krize se nebát požádat o konzultaci specializované instituce. Využít můžete např. online poradnu projektu E-Bezpečí na adrese www.napisnam.cz**
- .

Pro E-Bezpečí
Kamil Kopecký,
Univerzita Palackého v Olomouci