

PODVODY NA INTERNETU. Jak je odhalit, jak se proti nim bránit.

Podvody na internetu jsou často velice sofistikované. Policie upozorňuje, že jejich objasnění je komplikované. Pachatelé většinou působí ze zahraničí, využívají anonymního prostředí a šifrované komunikační kanály. Přesto se daří rozkrývat organizované skupiny, které mají na svědomí stovky skutků s milionovými škodami.

I já jsem se stal potenciální obětí pro podvodníky. Začalo to asi takto (*citace textu bez úprav*):

Já: Vložil jsem na inzertní portál <https://www.bazos.cz> inzerci, že prodávám elektrické topení a během hodiny jsem dostal odpověď.

Podvodník: Dobrý den, je Topení - Infračervený topný panel stále na prodej? Jsem Ze Stříbra.

Já: Jestli jste ze Stříbra, tak by bylo lepší si přijet. Na místě to vyzkoušíme, že je to funkční. A vy si to odvezete. Jen se mi nezdá Váš e mail. No, uvidíme.

Podvodník: Dobře. Udělám objednávku u kurýrní služby, abych vás této části procesu zbavil. Mám zkušenosti s DPD, takže bude nejlepší to zařídit přes ně. Nejprve obdržíte platbu prostřednictvím kurýrní služby na svůj účet, a poté vás bude kurýr kontaktovat telefonicky. Náklady na doručení samozřejmě hradím Já. Prosím, pošlete mi své údaje – adresu a telefonní číslo, na kterém vás může kurýr zastihnout. :)

Jako profesionál jsem odhadl, že se jedná o podvod. A komunikaci ukončil. Už e mail kuferiyuxu82@gmail.com byl velmi nedůvěryhodný.

Pro tyto podvodníky jsou bazary všeho druhu doslova zlatý důl. V posledních letech jsme svědky prudkého nárůstu kriminality páchaného v kybernetickém prostoru. Útoky pachatelů jsou čím dál promyšlenější a častější. V kyberprostoru je pachatel anonymní. Začíná to tak, že „zájemce“ pošle inzertnímu odkaz na přepravní službu GLS, DPD a podobné přepravní společnosti. Ovšem jedná se o podvrženou stránku. Inzerující si toho bohužel nevšimne. Stránku otevře a přihlásí se do svého internetového bankovníctví. Přijde mu kód, který potvrdí a tím si zadělá na problém.

V případě včasného zjištění je nutné si zablokovat svůj účet a platební kartu a informovat policii. Pokud to neuděláte, podvodník si požádá o vystavení další platební karty a účet okamžitě „vysaje“.

Jak se bránit?

Pokud je to jen trochu možné, požadujte osobní předání zboží. To je nejsnadnější způsob, jak na podvodníky vyvrát.

Nikdy nesdělujte podrobnosti a údaje ke svému bankovnímu účtu a jeho heslu, či klíči, číslu platební karty, CVC kódu a expiraci.

Snižte si limity pro platby a zejména pro platby po internetu, v případě nutnosti se tyto limity dají na počkání v bankovníctví navýšit

Podvodníci za sebe často nechají psát konverzaci tzv. Chatboty, tudíž preferujte osobní volání v GSM síti.

Neinstalujte si Vám neznámé aplikace do svých zařízení na doporučení neznámých osob, následkem může být nejen prázdný účet, ale i odcizená identita.

Nestahujte do svého telefonu aplikace pro vzdálenou správu, vzdálenou pomoc, on-line podpory, nebo prezentaci vzdálené plochy. Tyto softwary umožňují připojit se na

vzdálené zařízení, jako jsou počítače, servery, nebo mobilní zařízení, a to kdekoliv na světě. Jedná se například o AnyDesk, Chrome Remote Desktop- pokud má chrome, Splashtop, RemotePc. Pro iOS tady zařízení s jablkem je to ZohoAssist..... .

Nicméně běžné sdílení obrazovky je možné zapnout například i na Whats Appu a průšvih je na světě. Nejednejte s nikým po Whats Appu, Telegramu a podobných sociálních sítí, koho opravdu neznáte.

Do bankovníctví se přihlašujte zásadně z aplikace, kterou máte v zařízení uloženou, nikdy ne přes prohlížeč a na doporučení či radu neznámé osoby, mohlo by se totiž stát, že se nedobrovolně přihlásíte a zadáte své bankovní informace přímo pachateli a to aniž byste si to uvědomovali.

V případě podezření volejte ihned na linku 158 a do své banky. Zablokujte si účet!

Většina bankovních institucí nabízí pojištění internetových rizik, kdy pojištění pokryje podvody v případě, že poškozený nesdělil údaje o účtu a jeho zabezpečení.

Zpracoval: PhDr. Jaroslav Beneš a

por. Bc Eva Havelková DiS, specialistka přes kyberkriminalitu KŘ Policie ČR