

Upozornění na podvodná jednání

14.3.2024 - Zuzana Churaňová | Policie ČR

Budte obezřetní!

Policisté Krajského ředitelství policie Karlovarského kraje evidují od začátku roku několik desítek podvodných jednání. Scénář je téměř ve všech případech stejný. Podvodník se snaží ze svých obětí pod různými záminkami vylákat jejich naspořené finance. Ať už se vydává za jejich banku, nebo své oběti láká na „výhodné“ investice. Podvodných taktik je celá řada a oběti se může stát prakticky kdokoliv. Nejčastější jsou podvody na klienty bank, jako jsou např. podvodné e-maily tzv. phishing nebo podvodné SMS tzv. smishing.

Cílem těchto útoků je získat od obětí citlivé údaje o jejich bankovní kartě, internetovém bankovníctví či jiné citlivé informace nebo je navést na odkaz se škodlivým obsahem.

Další způsob, jak vylákat z obětí peníze je tzv. vishing. Tento způsob je nejzákeřnější, protože se jedná o telefonní hovor s živým člověkem, který chce svou oběť vystrašit a zároveň vzbudit důvěru, že je tím, kdo může pomoci. Pod záminkou napadení bankovního účtu, pomoci zraněnému příbuznému či ochrany peněz před podezřelými transakcemi nebo s nabídkou výhodných investic své oběti zavolá a tím, že se vydává např. za pracovníka banky, policistu apod. získá ve své oběti důvěru a pak už oběť jednoduše připraví o peníze.

Obdobný případ řeší v současné době karlovarští kriminalisté. Ženu z Karlovarska ve věku 35 let telefonicky kontaktoval z různých čísel neznámý pachatel, který se představil jako pracovník banky. Pod záminkou, že má žena napadený bankovní účet ji přiměl provést několik plateb. Poté ženu přemluvil k tomu, aby vybrala ze svého účtu více jak půl milionu korun a ty předala údajnému kurýrovi. Celkem tak žena přišla ze svých úspor o více jak 800 000,- Kč.

O více jak 120 000,- Kč přišla 49letá žena z Karlovarska. Neznámý pachatel uvedl poškozenou ženu v omyl a zamlčel podstatné skutečnosti. Poškozená žena měla na sociální síti kliknout na Bitcoinovou reklamu, přičemž po přesměrování uvedla své telefonní číslo. Poté jí kontaktoval údajný manažer a ženu přesvědčil o vložení vstupní investice v hodnotě několika tisíc korun, které mu žena z účtu odeslala. Po několika dnech jí kontaktovala jiná pracovnice, která pod smyšlenou záminkou chtěla po poškozené větší obnos peněz z důvodu stoupnutí ceny zlata, aby tak více vydělala. Poškozená žena však už žádné peníze neposlala a tak jí obelstili tím, že jí „jako“ půjčili do její virtuální peněženky 5 000,- dolarů a z těch vydělala 15 000 dolarů, ale těch půjčených 5 000 dolarů jim musí vrátit. A tak poškozená žena ze svého účtu odeslala částku více jak 4 500,- euro, přičemž tak celkem přišla o cca 125 000,- Kč.

Podvodníci neznají meze a jejich podvodné taktiky zkouší opravdu na každého. Příkladem je případ, kdy dosud neznámý pachatel poslal falešný e-mail účetní jedné z Mateřských škol na Karlovarsku, ve kterém se vydával za ředitelku této školky. V něm se dotazoval na aktuální zůstatek finančních prostředků na bankovním účtu a také možnost, zda by se mohlo z tohoto účtu odeslat více jak 23 000,- euro. Poté účetní zaslal všechny potřebné údaje k převodu peněz. Duchapřítomná účetní se spojila s ředitelkou školky a tím tak zjistila, že se jedná o podvod. Případem se v současné době zabývají policisté.

Jediný způsob jak se ubránit takovýmto podvodům, je být obezřetný. Pamatujte si, nikdy Vám nikdo nedá nic zadarmo. Nikdy nikomu nesdělujte své citlivé údaje, jako jsou přihlašovací údaje do internetového bankovníctví, údaje k platební kartě apod. – banky se **NIKDY** na tyto informace neptají!!! Nereagujte na telefonní hovory, e-maily ani zprávy, kde se Vás někdo pokouší

vmanipulovat do situace, že jsou Vaše finanční prostředky v ohrožení a Vy musíte udělat další kroky pro jejich záchranu - **KDYBY BYLY VAŠE PENÍZE V OHROŽENÍ, BANKA ZAREAGOVALA DÁVNO UŽ BEZ VÁS!!!**

V případě pochybností vždy kontaktujte svou banku či volejte na 158. Myslete na to, že útočník dokáže napodobit jakékoliv telefonní číslo či e-mail!!!

<https://www.policie.cz/clanek/upozorneni-na-podvodna-jednani.aspx>