

Zpravodajství v Ostravě

10.2.2023 - Eva Michalíková | Policie ČR

Opět další lidé uvěřili podvodníkům a přišli o peníze...

Policisté z oddělení hospodářské kriminality Ostrava prověřují další případy podvodů, kde modus operandi je sice jiný, ale výsledek je úplně stejný... důvěřivé osoby přišly o peníze a ještě si jeden z poškozených vzal úvěr.

V prvním případě 20letý muž přijal hovor od údajného pracovníka banky. Ten mu sdělil, že zmeškal osobní schůzku v bance, která měla být navazující na schůzku předchozího dne. Jakmile se 20letý muž ohradil, že v bance nemá ani vedený účet a že na žádné schůzce nebyl, reakce muže na druhé straně telefonu byla velice pohotová. Sdělil mu jméno, příjmení a dokonce i adresu, což opravdu vše souhlasilo a pokračoval tím, že došlo zřejmě ke zneužití jeho osoby a že věc předá policii. Dále se zeptal, kde má vedený účet a hovor ukončil. Následoval další hovor, tentokrát už údajně z banky, kde má poškozený vedený účet. „Pracovník banky“ mladíka informoval, že se stal obětí podvodníka a po celou dobu hovoru na něj naléhal, aby si vzal co nejvyšší možný úvěr, aby náhodou nedošlo k dalšímu zneužití. Mladík tedy poslechl, šel do banky v nákupním centru v Ostravě a sjednal úvěr ve výši 566.000,- Kč. Po celou dobu měl zapnutý telefon dle žádosti volajícího. Získané peníze z úvěru přišly na účet a následně mu bylo vysvětleno, jak splatit úvěr, aby byla u České národní banky nulová anulace pro poskytnutí úvěru a aby nedošlo k dalšímu zneužití osobních údajů poškozeného. Na to už poškozený reagoval nesouhlasně a „pracovníkovi banky“ sdělil, že s tímto postupem nesouhlasí a z nákupního centra odešel. Podvodníci se s tímto neztotožnili a pod další lží se s 20letým mladíkem spojili. Tentokrát to byl „údajný policista“ s vysokou hodností, který mu měl vysvětlit, že pro ochránění svých financí je musí vložit do bitcoinmatu. Sdělil mu, kam má jet a upozornil ho na to, že jinde peníze vkládat nesmí, jinak o ně přijde. Na základě zaslaných několika QR kódu poškozený postupně do bitcoinmatu vložil 315.000,- Kč. Zbylé peníze, které získal na úvěr už do bitcoinmatu nevložil s tím, že mu vše přišlo podezřelé. Proto se rozhodl jít osobně na policejní služebnu, kde se mu potvrdilo, že se stal obětí podvodu. I přesto, že během několika minut poškozený telefonicky kontaktoval osobu, která je uvedena na bitcoinmatu, tak pracovník jen potvrdil, že nákupy již byly provedeny a bitcoiny jsou na anonymních účtech.

I ve druhém případě 28letý poškozený uvěřil dalšímu muži po telefonu. Ten mu uvedl, že je zaměstnancem České národní banky a jeho účet byl napaden hackery a platební karta byla zavirovaná. Následovaly rady, jak bezpečně zajistit účet, aby nedošlo k odčerpání finančních prostředků. Poté následoval postup, co má dělat. Rada zněla: „Ze svého bankovního účtu převedte na „bezpečný“ účet své peníze a po odvirování budou vráceny zpět“. Poškozený souhlasil. Dle instrukcí si během hovoru nainstaloval do mobilního telefonu požadovanou aplikaci, která je určena pro vzdálený přístup. Následně přes aplikaci neznámému pachateli umožnil náhled na svou platební kartu, přičemž mu sdělil i číselný kód pro autorizaci on-line plateb (kód CCV). Pak už jen muži po telefonu sdělil několik potvrzujících peněžních transakcí, sám je v internetovém bankovníctví potvrdil, načež jeho účet byl během okamžiku „lehčí“ o téměř 200.000,- Kč.

Co z toho plyne a co bychom chtěli znovu připomenout:

Kybernetická kriminalita již dávno necílí jen na seniory a osamělé lidi, ale pachatelé se zaměřují na širokou veřejnost bez ohledu na věk či vzdělání. Počet útoků na klienty bank se za poslední dva roky zvýšil čtyřnásobně a škody jdou do stovek milionů.

Pachatelé se při těchto útocích snaží překonávat zejména lidský faktor a pod nejrůznějšími

legendami využívají nátlaku, strachu a časové tísně pro záchranu peněz nebo pro realizaci finanční transakce. Mezi nejčastější podvodné legendy patří:

Podvodné navolávání: pachatelé se vydávají například za bankéře, policisty, pracovníky technické podpory a snaží se z lidí pod vlivem strachu vylákat peníze, nebo vzdálený přístup do zařízení oběti, který následně zneužije.

Nabídka výhodných investic: přesvědčivá lákavá reklama a manipulativní jednání. Cílem pachatele je vylákat z oběti co možná nejvíce finančních prostředků a využívá k tomu přirozenou ziskuchtivost každého z nás.

Základní rady, jak nenaletět:

Nikdy neumožňuj vzdálený přístup do svého zařízení nikomu, koho neznáš a zcela mu nedůvěřuješ.

Pamatuj si, že pachatelé dokáží napodobit jakékoliv telefonní číslo, či e-mailovou adresu.

Jedním ze základních pravidel je nikdy nikomu nesdělovat hesla k internetovému bankovníctví.

Na podezřelé SMS zprávy nikdy nereagujte. Vaše banka by po vás přístupové údaje či hesla skrze SMS zprávu nikdy nepožadovala.

Naletěli jste podvodníkovi, klikli jste na falešný e-mail nebo jste někomu sdělili své údaje? Ihned zavolejte kontaktnímu centru své banky a požádejte o zablokování on-line bankovníctví a o změnu přihlašovacích údajů. Vše ihned ohlaste na policii.

Policisté Krajského ředitelství policie Moravskoslezského kraje pro Vás připravili nové edukační video zaměřené na podvody v a trestné činy spojených se zneužitím důvěry osob, které měly zájem investovat do kryptoměn. Jedná se o video z preventivního projektu s názvem „PORADCE policejní rádce pro bezpečný život“.

https://www.youtube.com/watch?v=KrfSfIVycYo&list=PL7q4z0ZRpaLBLvhCrDvKKnEO-TAtCVoHx&index=17&ab_channel=Policie%C4%8CR

<https://www.policie.cz/clanek/zpravodajstvi-v-ostrove-745024.aspx>