

Internetoví podvodníci přitvrzují

22.10.2024 - Simona Vacherlohnová | Policie ČR

Falešný bankéř díky promyšlené legendě připravil ženu o 400 000 korun. Přečtěte si jak nad podobnými podvodníky vyzrát a buďte připraveni.

Berounští policisté od 16. října prověřují podvodné vylákání peněz. Na služebnu do Berouna se dostavila paní, která oznámila, že jí telefonicky kontaktovala žena, která se představila jako pracovnice banky. Následně si volající jménem, příjmením a datem narození ověřila u ženy její totožnost. Tyto údaje měla „bankérka“ správné, čímž u ženy, které volala, zvýšila její důvěryhodnost. Po ověření údajů se ženy dotázala, z jakého důvodu se nedostavila na sjednanou schůzku. Překvapená žena o žádné schůzce nevěděla, a tak se začala o situaci dále zajímat. Falešná bankérka ženě vysvětlila, že se někdo pokusil na ženu sjednat spotřebitelský úvěr a že žadatel zneužil její údaje. Bankérka přepojila ženu na „bezpečnostního technika“, který jí doporučil převedení finančních prostředků na zrcadlové účty, což žena na základě doporučení a naléhání provedla. Následně dle pokynů převedla své finanční prostředky ve výši 400 000 korun na zadané čísla účtů. Od pracovníka banky obdržela přístupové údaje do zrcadlových účtů a informaci, že se jí brzy ozve Policie ČR. Přístupy nefungovaly, Policie ČR se neozvala a ženě tak nezbývalo nic jiného než se obrátit na svou banku, kde jí sdělili, že se stala další obětí podvodníků.

V tomto případě sehrál významnou roli fakt, že vystupující podvodnice znala osobní údaje osoby, které volala, což zásadně zvýšilo důvěryhodnost telefonátu. Mezi další nástroje podvodníků patří naléhání, časová tíseň a strach, který vyvolávají. Sofistikovanější technikou je **spoofing**. Jedná se o zneužití oficiálních telefonních čísel bank a dalších institucí. To znamená, že u příchozího hovoru vidíte známé telefonní číslo, ve skutečnosti ale volá kdo cizí. Tento způsob využívají často podvodníci, kteří se vydávají za pracovníky bankovních institucí, za policisty a další úředníky. Přečtěte si více o podvodných technikách a buďte připraveni.

Jak se proti případným podvodům bránit?

Nereagujte na podobné hovory a v žádném případě nesdělujte k Vaší osobě žádné citlivé údaje ani bezpečnostní údaje z vaší platební karty, nebo přístupové údaje k online bankovníctví.

Veškeré informace o napadení účtu atp. si před tím, než provedete nenávratný krok, ověřte u své banky, a to telefonicky na oficiálních telefonních číslech nebo osobně na pobočce banky. Nenechte se zmanipulovat strachem, časovou tísni a dalším nátlakem!

Nikdy nikomu nesdělujte a ani nepřeposílejte bezpečnostní / autorizační kód, který Vám přišel formou SMS zprávy.

Myslete na to, že útočník dokáže napodobit jakékoliv telefonní číslo, odesílatele SMS zprávy, ale třeba i e-mailovou adresu.

Nikdy nikomu nedůvěryhodnému neumožňujte vzdálený přístup do Vašeho počítače.

Sledujte a pečlivě čtěte informace od Vaší banky v internetovém bankovníctví.

Při každém vstupu do internetového bankovníctví kontrolujte, zda odpovídá doména přihlašovací stránky. Toto platí vždy, když někam zadáváte své osobní nebo přihlašovací údaje. Pamatujte, že nejbezpečnější přihlášení do internetového bankovníctví je přes

mobilní aplikaci.

Aktualizujte software, antivirový program, firewall v zařízení, ze kterého do vstupujete do internetového bankovníctví.

Během, nebo po takovémto podezřelém hovoru, si zaznamenejte údaje, které Vám útočník sdělil (jména, e-mailové adresy, čísla účtů, odkazy na webové stránky, apod.) a neprodleně kontaktujte Policii ČR na lince 158 i bankovní instituci, případně se pokuste probíhající hovor zaznamenat.

<https://www.policie.cz/clanek/internetovi-podvodnici-pritvrzuji.aspx>