Další podvody falešných bankéřů

15.9.2023 - Miroslava Glogovská | Policie ČR

Poškození uvěřili a přišli o více než 200 tisíc korun.

Další dva podvody s využitím legendy „falešného bankéře“ byly v posledních dnech oznámeny chomutovským policistům. Poškození, kteří podvodníkům naletěli, tak přišli v součtu o více než 200 tisíc korun.

Jako první se na chomutovské obvodní oddělení obrátila 37letá žena. Na její telefon volal muž, který se představil jako pracovník České národní banky a sdělil jí, že došlo k napadení jejího bankovního účtu. Pokud prý chce své peníze zachránit, musí je přeposlat na jiný účet, jehož číslo jí nadiktoval. Žena dotyčnému uvěřila a ve třech platbách mu odeslala celkem téměř 150 tisíc korun.

Případ téměř jako „přes kopírák“ si policisté na stejném oddělení vyslechli jen o tři dny později. Pětaosmdesátiletému seniorovi zavolal údajný zaměstnanec České národní banky s tím, že došlo k napadení jeho účtu. Aby ochránil své finanční prostředky, musí je zaslat na stanovený bankovní účet. Na pokyn falešného bankéře si pak stáhnul aplikaci sloužící pro vzdálený přístup. Z té potom volajícímu nadiktoval kód, kterým se následně podvodník spároval s jeho mobilem. V mobilním bankovnictví pak zadal tři odchozí platby, které mu navíc senior potvrdil zaslaným PIN kódem. Přišel tak o částku přesahující 55 tisíc korun.

VISHING

VOLÁ VÁM BANKOVNÍ ÚŘEDNÍK A TVRDÍ, ŽE JE VÁŠ ÚČET V OHROŽENÍ, A ŽE MÁTE OKAMŽITĚ SVÉ PENÍZE POSLAT JINAM? ZBYSTŘETE. SKUTEČNÍ BANKOVNÍ ÚŘEDNÍCI TAK NIKDY NEPOSTUPUJÍ.

VISHING neboli také podvodné navolávání patří mezi další triky podvodníků. Není už žádnou novinkou, ale raději si připomeneme, v čem spočívá.

Pachatelé se vydávají za bankéře, případně policisty, oslovují oběť s legendou napadení jejího účtu a vybízejí k rychlému zálohování peněz, včetně přesných instrukcí, kam finanční prostředky ukrýt.

Oběť je zmanipulována k převodu finančních prostředků, k výběru a vložení finančních prostředků do vkladomatu na virtuální měnu nebo k vyzrazení citlivých údajů a případně k umožnění vzdáleného přístupu do svého zařízení.

Útočník často používá tzv. spoofing, to znamená, že telefonní číslo volajícího se tváří jako regulérní telefonní číslo banky, Policie ČR nebo jiným důvěryhodných institucí. Podvodníci v těchto případech dokáží napodobit jakékoliv telefonní číslo.

Nezapomínejte, že banka dokáže vaše peníze ochránit sama, pokud zjistí podezřelou aktivitu. Nikdy proto nebude požadovat, aby klient prováděl jakýkoliv převod nebo aby poskytl vzdálený přístup do mobilního telefonu nebo počítače.

Banka nikdy po klientovi nevyžaduje telefonicky citlivé údaje, kopie dokladů a platební karty. Všechny tyto údaje už o svých klientech má.

V případě podezření na podvod okamžitě kontaktujte svou banku.

http://www.policie.cz/clanek/dalsi-podvody-falesnych-bankeru.aspx