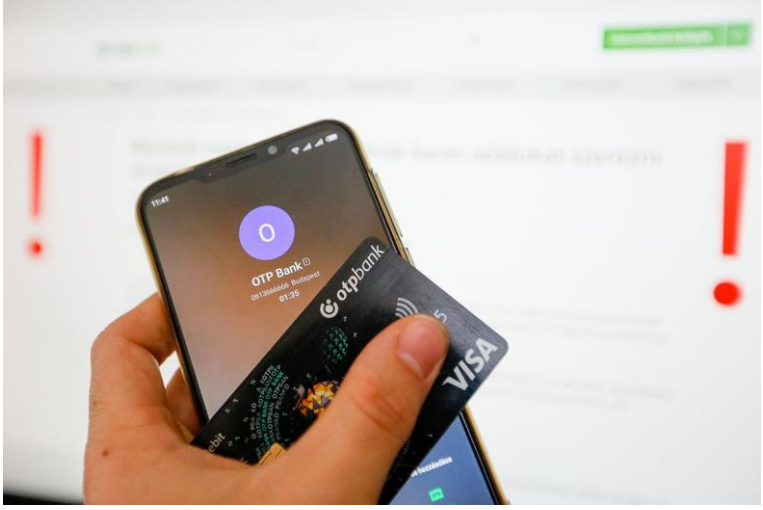
ELBIR

Elektronikus Lakossági Bűnmegelőzési Információs Rendszer

Hogyan ne váljunk magukat banki alkalmazottnak kiadó csalók áldozatává



forrás:internet

A telefonos csalásoknak egyik típusa, amikor a csalók magukat banki alkalmazottnak kiadva, gyanús tranzakciók miatt keresnek meg bennünket. A hívás nem egyszer olyan bank nevében érkezik, ahol nem is vezetünk számlát. Amint ez kiderül a csaló azonnal „intézkedik” és „átkapcsol” a számlavezető bankhoz. A csalók a pénzünk visszaszerzése, a tranzakciók megakadályozása, a bűncselekmény elkövetőinek kézre kerítése érdekében kérik közreműködésünket. Valódi szándékuk azonban a személyes és banki adataink, a fizetési művelet jóváhagyásához szükséges kódok megszerzése.
A telefonhívások többségében egy **távoli hozzáférést biztosító alkalmazás** (jellemzően AnyDesk, TeamViewer, RustDesk) telepítését is kérik tőlünk. A cél az, hogy a csaló hozzáférjen az adott eszközön elérhető adatokhoz, az általa szándékolt fizetési műveletek, átutalásokra kerüljön sor.
Gyakori, hogy a csaló azzal hiteget bennünket, hogy a gyanús tranzakció összegét másnap vagy egy későbbi időpontban visszakapjuk, addig ne keressük sem a bankunkat, sem a rendőrséget. A banki ügyintézők, rendőrök is érintettek a csalásban, és az ügy felderítése érdekében tilos bárkivel is beszélnünk a történtekről. A valódi cél azonban az, hogy minél később tegyünk bejelentést a bankunknál és a rendőrségen.

Néhány jó tanács, ami alapján gyanítható, hogy csalóval van dolgunk:
- A bankok ügyfélszolgálatai a valóságban nem kapcsolják át a hívást sem más bankhoz, sem a rendőrséghez.
- Nem biztos, hogy a bank alkalmazottjával beszélünk, ha látszólag a számlavezető bank telefonszámáról érkezik a hívás. Ismert elkövetési mód ugyanis a **hívószám-hamisítás (spoofing)** útján elkövetett csalás is.
- A csalók sokszor sürgető, akár fenyegető hangnemet alkalmaznak.
- A bank soha nem kéri semmilyen alkalmazás letöltését, nem kéri PIN kódunkat vagy sms-ben küldött kódokat.

Tolna Vármegyei Rendőr-főkapitányság
Bűnmegelőzési Alosztály
7100 Szekszárd, Mészáros L. u. 19-21.
bunmegelozes.tolnavmrfk@tolna.police.hu

- Ellenőrizzük rendszeresen bankszámláinkat, és figyeljük a gyanús tranzakciókat. Ha olyat találunk, amit nem mi kezdeményeztünk, a banki ügyintéző azonnal letiltja internetbankunkat, bankkártyánkat, ha elmondjuk, hogy a gyanús műveletet nem mi végeztük.
- Ha kételyünk van, éljünk akár a keresztazonosítás lehetőségével. Ennek során legalább három kérdésre részben az ügyfél, részben a szolgáltató ügyintézője válaszol a beszélgetésben. Ez a gyakorlatban azt jelenti, hogy az ügyintéző által feltett biztonsági kérdésekre (pl. anyja neve) a válaszok egyik felét az ügyintéző adja meg, a válaszok másik felét pedig mi.

Ha mégis megtörtént a baj, haladéktalanul vegyük fel bankunkkal a kapcsolatot és tegyünk rendőrségi feljelentést. A rendőrség foglalhatja le azt a bankszámlát, amire a pénzünket átutalták, a bankunknak nincs ilyen jogosítványa.

Az érintettek áldozatvédelemmel kapcsolatos információkért, bűnmegelőzési tanácsokért fordulhatnak személyesen és telefonon is a Tolna Vármegyei Rendőr- főkapitányság Bűnmegelőzési Alosztály, illetve a városi rendőrkapitányságok munkatársaihoz, illetve írhatnak a kiberkapcsolat@tolna.police.hu e-mail címre is.

Ha bajba kerül, forduljon a rendőrséghez, vagy hívja a 112-es segélyhívó számot!

Tolna Vármegyei Rendőr-főkapitányság
Bűnmegelőzési Alosztály
7100 Szekszárd, Mészáros L. u. 19-21.
bunmegelozes.tolnavmrfk@tolna.police.hu