ELBIR

Elektronikus Lakossági Bűnmegelőzési Információs Rendszer

HISZÉKENYSÉG, KONTRA VÉDELMI FUNKCIÓK

Digitális világban élünk, internet nélkül szinte el sem tudjuk már képzelni az életünket. Online vásárolunk, online bankolunk, online tartjuk a kapcsolatot a családdal, ismerősökkel, szükség esetén az iskolával, a munkahelyünkkel. Tisztában kell lennünk e világ veszélyeivel és fel kell rá készülnünk!

A különböző internetes biztonsági kódok, erős banki ügyfélhitelesítés világában felmerülhet, hogy miként valósulhatnak meg egyáltalán a visszaélések. A Pénzügyi Békéltető Testülethez (PBT) beérkező panaszok alapján sokszor úgy, hogy a jóhiszeműségre és a tájékozatlanságra alapozva - ugyanakkor a körülmények által nem indokoltan - pszichológiai nyomás alá helyezik az ügyfelet egy-egy csalárd telefonhívás alkalmával.

Egyre gyakrabban fordul elő, hogy az ügyfelet ráveszik, hogy a mobiltelefonra töltsön le távoli hozzáférést biztosító alkalmazást, melynek segítségével a csalók megismerhetik az SMS-ben kapott biztonsági kódot, és a banki alkalmazások felett át tudják venni az irányítást. A PBT tapasztalatai szerint sok esetben még erre sem volt szükség, mert a hiszékeny ügyfelek a csalók kérésére az SMS-ben szereplő kódokat maguk adták ki, vagy a mobilalkalmazásban elvégzett hitelesítésekkel a tranzakciókat maguk hagyták jóvá.

Az ügyfelek az elkövetők által kért tranzakciót megelőzően látták annak minden adatát: a kedvezményezett nevét, a tranzakció összegét és devizanemét, mégsem fogtak gyanút. A csalók a bankkártya valamennyi adatának kiadása mellett a kód elárulására is rávették az ügyfeleket, ami állításuk szerint azért volt szükséges, mert a tranzakció ügyfél általi jóváhagyásával a tranzakciót zárolták, blokkolták vagy az adott összeget „biztonságos rendőrségi számlára” helyezték. A kontrollszolgáltatással rendelkező ügyfelek a művelet után rögtön észlelték a számlaegyenlegük csökkenését. Az ő kételyeiket azzal hárították el, hogy a pénzt átmenetileg védelem alá helyezték, és majd a bank később visszavezeti azt a „biztonsági számláról”. A csalók fő érve tehát az volt, hogy az ügyfelek pénzét védik, de valójában éppen elvették azt!

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

Mit lehet tenni a telefonos csalók ellen?

A bankok saját internetes felületükön, e-mailen, netbankon vagy a banki mobil alkalmazáson keresztül küldött push üzenetben folyamatosan tájékoztatják ügyfeleiket az aktuális adathalász kísérletekről, banki csalásokra használt módszerekről. Ne sajnáljuk az időt a banktól kapott üzenetek átolvasására! Ellenőrizzük, hogy az SMS-en vagy mobilalkalmazáson keresztül kapott üzenet tartalma, az abban szereplő tranzakció valóban megfelel a szándékunknak. Legyünk körültekintők! Minden szempontból megéri.

Szólaljon meg a belső vészcsengője! Szakítsa meg a hívást, és tárcsázza a bankját, ha hasonló gyanús telefonhívással, sürgető hangnemben próbálják rávenni személyes ill. érzékeny banki adatainak, kódjainak megadására, vagy ismeretlen alkalmazás letöltésére.

További hasznos információk a kiberpajzs.hu oldalon!

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