ELBIR

Elektronikus Lakossági Bűnmegelőzési Információs Rendszer

Egyre gyakoribbá váltak az online csalások!
Ön ne váljon áldozattá!
Kérjük, olvassa el és fogadja meg tanácsainkat!

Az ún. **„banki ügyintézős” csaláskor** az elkövetők egyike bankbiztonsági szakembernek adja ki magát és azzal hívja fel a sértettet, hogy a bankszámláján jogosulatlan tranzakciók történtek.
Az elkövető célja, hogy megszerezze a sértett online vásárláshoz szükséges bankkártya adatait, illetve a netbank belépéshez szükséges azonosító adatait. Jellemző, hogy az elkövetők rendkívül elszántak és kitartóak, akár több órás, hitelesnek tűnő beszélgetéseket folytatnak a sértettekkel amivel elnyerik a bizalmukat.

A bankok telefonon nem kérnek bankkártya adatokat, illetve internetes belépési adatokat az ügyfelektől, így ha ilyen adatokat kér a telefonáló, kezdjünk gyanakodni!

„Ügyintézőnek” telefonon ne adjunk meg bankkártyaadatot!
„Ügyintézőnek” telefonon ne adjunk meg internetes belépési adatot!
Internetbankolásra a bank applikációját használjuk!

A **„hamis link” módszer** lényege, hogy az elkövetők a bank hivatalos webcíméhez nagymértékben hasonlító, attól akár csak 1-2 karakterben eltérő webcímű ál-banki oldalt hoznak létre.
Amikor a sértett az internetes keresőbe begépeli a bank nevét, a találatok között elsőként a hamis banki oldal linkje jelenik meg. A sértett erre rákattint, majd abban a hitben van, hogy a bankja hivatalos felületén ad meg adatokat. Valójában azok nem a bank rendszerében jelennek meg, hanem az elkövetők látják. A bűnözők párhuzamosan, azonos időben belépnek a sértett valódi banki oldalára ahol az azonosító adatokat, jelszót, valamint az egyedi, megerősítő SMS kódot is beírják, és már hozzá is férnek a sértett bankszámlájához és banki fiókjához.

A webcím melletti lakat ikonra kattintva ellenőrizzük, hogy biztonságos-e az oldal!
Magyartalan kifejezésekre figyeljünk fel!
Ha pénzt várunk ne adjuk meg a pénz küldőjének a bankkártya adatainkat!

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

Az **„apróhirdetéses csalás” módszer** lényege, hogy a sértett online apróhirdetési oldalon árul valamit, az elkövető pedig – csevegő alkalmazáson keresztül – mint vásárló keresi fel őt. A csaló ezután azt javasolja az eladónak, hogy csomagküldő szolgálatot vegyenek igénybe, ehhez küld neki egy linket azzal, hogy azon keresztül kapja majd meg a vételárat is. A link egy ismert csomagküldő szolgálatéhoz hasonló hamis oldalra vezeti a sértettet, akinek ott ki kell választania a számlavezető bankját, majd ezután egy felugró ablakban meg kell adnia a bankkártyája valamennyi adatát - a CVC biztonsági kódot is beleérve.

Mindezzel a sértett tudtán kívül az elkövető rendelkezésére bocsátja az adatait, aki azokkal online vásárlást indít. A sértett közben egy másik felugró ablakban megadja a telefonjára érkezett SMS kódot is, amit az elkövető már az online vásárlási felületen rögzít.

Előfordul, hogy az elkövetők nem csomagküldő szolgálatra hivatkoznak, hanem azt közlik, hogy közvetlenül a hirdetési oldalon keresztül küldik el a vételárat, és annak fogadásához küldenek linket.

Fontos, hogy hirdetési ügyletek során ne kattintsunk az állítólagos vevő által küldött linkekre és eleve legyen gyanús az, hogy ha pénzt várunk, akkor a bankszámlaszámunk helyett miért kérik tőlünk a bankkártya adatainkat. Jellemző és gyanúra okot adó körülmény az is, hogy a hamis weboldalak rendszerint magyartalan kifejezéseket használnak.

A **„nyereményjáték” módszer** lényege, hogy az elkövetők nyereményjátékra hivatkoznak és így szerzik meg a sértettek bankkártya adatait vagy arra veszik rá áldozataikat, hogy kisebb összegű regisztrációs díjat fizessenek a nyereményük kiutalása érdekében.

Ha pénzt várunk, akkor ne adjuk meg a bankkártya adatainkat és ne utaljuk pénzt arra, hogy megkapjunk egy ajándékot.

Az ún. **„ráijesztős” módszerrel** elkövetett csalások is terjednek. Ennél a módszernél az elkövetők chatben, sms-ben, vagy emailben rendszerint valamilyen felszólítást vagy figyelmeztetést küldenek, például streaming szolgáltató vagy hatóság nevében. Ezek a levelek vagy üzenetek szólhatnak arról, hogy a szolgáltató nem tudta levonni az előfizetést, ezért egy küldött linken belépési és bankkártya adatokat kér, vagy ha hatóság nevében próbálkoznak a csalók, akkor jellemzően valamilyen idézésre vagy felszólításra hivatkoznak, amit a káros linkre kattintva lehet elérni.

Gyanakodjunk, ha váratlan felszólítást kapunk. Ha elektronikus levelet kapunk mindig ellenőrizzük a feladót. A kifejezések általában magyartalanok, helyesírási és fogalmazási hibák szerepelnek a mondatokban, ezért eleve legyen gyanús a nyelvtanilag helytelen, magyartalan megfogalmazás. Soha ne kattintsunk csatolmányokra, linkekre megszokásból, mindig legyünk körültekintőek.

Az ismertetett elkövetési módszerek közös jellemzője, hogy az eldobható SIM kártyák vagy azonosíthatatlan IP, illetve e-mail címek mögé bújó csalók kilétének felderítése bonyolult feladat, ezért kiemelten fontos hangsúlyt helyezni ezeknek a bűncselekményeknek a megelőzésére, amelyhez fokozott körültekintésre és elővigyázatosságra van szükség.

Bűncselekmény elkövetése során forduljon a rendőrséghez és haladéktalanul tegyen feljelentést!

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