ELBIR

Elektronikus Lakossági Bűnmegelőzési Információs Rendszer

A pénzünkre és az adatainkra is utaznak a csalók

A csalók nagyon figyelik az aktualitásokat, banki átalakításokat, trendeket, időszakokat, a jogszabályváltozásokat, sőt még a jótékonysági akciókat is például háború, vagy földrengés kapcsán, és ezekre építik a legújabb megtévesztéses csalási módszereket.

Ki kell emelni az online csomagküldési szolgáltatókhoz, online piactérhez, webáruházakhoz kapcsolódó átveréseket. – Amíg pár éve még a vevőket károsították meg, most már az eladókat is.
A vevőnek álcázott csaló állítása szerint már kifizetett egy meghirdetett terméket, és az átutalás fogadásához kér programtelepítést: a leggyakoribb programok között van az AnyDesk, a TeamViewer és a RustDesk. Ha ezeket halljuk, mindjárt ugorjon fel egy kérdőjel, szólaljon meg a vészcsengő, mert ha telepítjük őket, azzal hozzáférést adhatunk az eszközünkhöz, üzeneteinkhez, és átadhatjuk az adatainkat – és velük az irányítást is – a csalónak!

Jellemző csalási módszer, amikor az eladó egy sms-t kap arról, hogy már kifizették az összeget, de a pénz átvételéhez meg kell nyitnia az üzenetben lévő linket. – „Már megérkezett a pénz, csak jóvá kell hagyni” – ILYEN NINCS! Ahhoz nem kell belépni a netbankunkba, hogy bármilyen összeget fogadjunk! Az elkövető célja ezekben az esetekben is az adataink megszerzése: ténylegesen a valódi banki oldalak másolata jelenik meg, ahol a saját bankomat ki tudom választani. Amikor azonban oda belépek, már a csalónak adom át az adataimat, amikkel ezután ő vissza tud élni. Az is gyakori módszer, hogy a „vevő” egy csomagküldő szolgáltatót ajánl a termékkiszállításhoz, szintén egy hivatkozással: de ha arra ráklikkelünk, egy hamis másolt oldalon a csalónak adjuk ki az adatainkat.

Még mindig jelen vannak az internetes vásárlásokra korábban jellemző átverések, amikor a megrendelt termék helyett valami rosszabb minőségűt vagy semmit sem küldenek az elutalt pénzünkért. Illetve előfordul, hogy kizárólag az adataink ellopása a célja a csalónak. Utóbbi esetben a csalók a bankkártyaadatainkat szerzik meg, így nem csak a „megvásárolt áru értékével”, hanem azon túl is jelentős összeggel károsodhatunk.

Fogadják meg bűnmegelőzési tanácsainkat:

Pénzösszeg fogadásához a nevünkön, számlaszámunkon, esetleg e-mail címen, telefonszámon kívül másra nincs szükség, ha valakinek ez nem elég, akkor azonnal szakítsuk meg vele a kapcsolatot!

Soha ne adjuk ki telefonon internetbanki azonosítóinkat, fizetéshez szükséges bankkártyaadatainkat! A bankkártya azonosító, az érvényességi idő és a háromjegyű CVC kód segítségével hozzáférhetnek pénzünkhöz.

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

Más kérésére semmilyen alkalmazást, programot ne telepítsünk a számítógépre vagy mobiltelefonra, még akkor sem, ha azt a bank vagy szolgáltató nevében kérik!

Online Piactéren soha ne fizessünk, ha mi vagyunk az eladók!

Online vásárlás esetén lehetőleg kizárólag az erre létesített, feltöltött virtuális kártyát, webkártyát használjunk. Ezen csak alacsony összeget tartsunk, illetve minden esetben mérlegeljük az előrefizetés kockázatát, legyen gyanús, ha utánvétre nincs lehetőség!

Kérjünk értesítést a bankunktól a számlánkat vagy kártyánkat érintő műveletekről, pénzmozgásokról, továbbá állítsunk be limiteket, regionális és online korlátozást bankkártyáinkra!

Mindig nézzünk utána, ellenőrizzük az adott oldalt, mielőtt vásárolnánk, nem valószínű, hogy mi leszünk az elsők, akit megpróbálnak átverni, és ennek általában nyoma van az Interneten.

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