

Biztonsági figyelmeztetést küld az Erste

Honlapján, közösségi oldalain, George Appban és George Weben, valamint ügyfeleinek küldött külön körlevélben hívja fel a figyelmet a banki adatok védelmére és egy, az elmúlt időszakban megszorodó csalástípusra az Erste. A csalók egy külön program telepítésére kérik áldozataikat, akik így maguk adnak hozzáférést a saját mobiltelefonjukhoz, számítógépükhöz. A bűnözők a szoftverrel átveszik az irányítást a készülékek felett, és lenullázzák a bankszámlákat. Az Erste a tájékoztatóban azt is összeszedte, mit tehetnek az ügyfelek, hogy pénzüket továbbra is biztonságban legyen.

Robbanásszerűen nőtt az elmúlt időszakban az egyik, banki ügyfeleket célzó csalástípus. Az általában magukat banki alkalmazottnak kiadó, vagy egyéb ismert cég nevében telefonáló csalók azzal jelentkezik, hogy gyanús tevékenységet látnak az ügyfél számláján, feltörték a felhasználói fiókját. Az ügyintéző azt kéri, az ügyfél telepítsen egy alkalmazást (például Anydesk, Teamviewer, RustDesk) a telefonjára és a számítógépére a helyreállítás, a károk elkerülése érdekében.

Amennyiben valaki letölt egy ilyen programot, azzal lehetővé teszi, hogy a bűnözők lássák, milyen kódokkal lép be a netbanki vagy mobilbanki felületre. Ezen kívül a csalók teljesen át tudják venni az irányítást a számítógép és mobiltelefon felett, az áldozat pedig ezután már csak tehetetlenül nézheti, hogyan szolgálgják ki magukat a bűnözők az ő számlájáról és utalják el maguknak a pénzt.

Az Erste már a csalások 90 százalékát ki tudja szűrni: a bank a tavalyi harmadik negyedévben összesen 4,4 milliárd forint ellopását akadályozta meg, ami majdnem a háromszorosa az első negyedéves összegnek. Ám hiába minden banki védelem, ha az ügyfél maga adja oda a kódokat a csalóknak. A tavalyi pénzügyi visszaélésekkel okozott ügyfélveszteség felét az említett módszerrel (Anydesk, vagy hasonló program telepítése) okozták a bűnözők. A lakás kulcsait se adjuk oda bárkinek, és nem adjuk oda a mobilunkat egy idegennek az utcán: nem szabad hozzáférést engedni a belépési kódokhoz, jelszavakhoz sem másoknak.

Az Erste most honlapján, közösségi oldalain, George Appban és George Weben, valamint tájékoztató levélben hívja fel az ügyfelek figyelmét az utóbbi időszakban megszorodó visszaélési kísérletekre. A bank a levélben tanácsokkal is segít abban, hogyan védekezhetnek ügyfelei a csalások ellen.

Az Erste tanácsai - Így védheted meg a pénzed!

- Banki adataid, mint a felhasználóneved, e-csatorna azonosítód, bankkártyád PIN-kódja vagy éppen CVV/CVC számod csak a tiéd. Maradjon is így, ne oszd meg senkivel!
- Sosem tudhatod, ki van a vonal másik végén. De azt tudd, hogy a bankok alkalmazottai soha nem kérnek arra, hogy bármit letölts a készülékedre! Ne tölts le semmilyen alkalmazást csak azért, mert egy telefonáló arra kér!
- Ha azzal hívnak, hogy felhasználói fiókodat, banki felületedet feltörték, illetéktelen utalások történtek, és azt kérik, hogy tölts le egy alkalmazást, azonnal szakítsd meg a hívást!
- Nem tudhatod, hogy milyen információkat szereztek meg rólad a csalók. Lehet, hogy tudják a neved, akár a számlavezető bankod is. De légy résen, fogadd meg tanácsainkat, ismerd fel, ha csalók keresnek!
- Soha ne utald el a számládon levő pénzt állítólagos biztonsági számlára, ha arra kérnek, hiszen a bankok ilyet soha nem tesznek!
- A bank, amikor csak lehet, igyekszik téged és a pénzed megvédeni, ezért csalás gyanúja esetén azonnal blokkoljuk a számlád és a kártyád használatát, és ezt követően megpróbáljuk felvenni veled a kapcsolatot. Mi nem fogunk téged sürgetni, főleg nem átkapcsolni hívás közben egy másik bankhoz.

Sajtókapcsolat:

- Pálosi Márta, szenior kommunikációs szakértő
- marta.palosi@erstebank.hu

Eredeti tartalom: Erste Bank Hungary Zrt.

Továbbította: Helló Sajtó! Üzleti Sajtószolgálat

Ez a sajtóközlemény a következő linken érhető el:

<https://hellosajto.hu/10725/biztonsagi-figyelmeztetest-kuld-az-erste/>