

Bűnmegelőzési hírlevél

Vigyázat, csalók! Válogatás az elmúlt hetek eseményeiből

Nagyon gyakori, hogy az elkövetők pénzügyintézetre, bankra hivatkozva csalják ki a számla vagy bankkártya birtokos személyes adatait, internetbanki belépéshez szükséges azonosítót, biztonsági kódot, jelszót vagy bankkártya adatokat.

Viszonylag új módszer, hogy a csalók a bankok, pénzügyintézetek web oldalaihoz a megszólalásig hasonlító ál web oldalakat hoznak létre, ahová egy, a bank nevében e-mailben küldött linkre kattintva lehet jutni, vagy a keresőbe beírva a keresett bank nevét, a felkínált lehetőségek között szinte bizonyosan az elsők között fog szerepelni az ál banki oldal is.

H.L. 2023.01.5-én egy telefonhívást kapott napközben, amelyben az ismeretlen telefonáló az MKB bank alkalmazottjaként mutatkozott be és banknál történt rendszer hibára hivatkozva különböző adategyeztetést kért. Sajnos a sértett megadta a kért adatokat, ezt követően a számlájáról több, mint 3,5 millió forintot utaltak el.

2023.01.23-án egy Gyöngyös környéki lakos az internetes címére egy adategyeztetésről szóló e-mailt kapott az MKB Bank nevében. Az e-mailben egy linket is küldtek, amely a bank oldalára navigálja. A linkre kattintva egy, a bank valódi oldalához a megszólalásig hasonlító oldalra került, ahol megadta a belépéshez szükséges adatait. Ezt követően rövid időn belül kapott a bankjától a mobil telefonjára egy ellenőrző hívást, amely szerint több, mint négy millió forintot utaltak el a számlájáról, mindezt a tudta és beleegyezése nélkül.

K.Ané adatait szintén egy, a bank nevében küldött linkre kattintva szerezték meg, amelyet e-mailban kapott. Tőle kérték a netbankos jelszava megváltoztatását is, amelyet követően a számlájáról közel 140 ezer forintot utaltak el.

Se szeri, se száma a hasonló eseteknek, kitől több, kitől kevesebb pénzt elutalva, elvásárolva a sértett bankszámlájáról a tudta és beleegyezése nélkül. Ami mindegyik esetben közös, a csalások elkövetéséhez a sértettek maguk szolgáltatották ki azokat adatait, amelyek birtokában lehetővé vált a bűncselekmények elkövetése.

- **Ne üzenetben kapott linkről lépjen a bankja web oldalára!**
- **Mindig ellenőrizze gondosan, hogy valóban a bankja hivatalos web oldalára lépett be!**
- **Üzenetben kapott linkről, vagy ismeretlen telefonáló által javasoltak alapján, még ha pénzügyintézeti alkalmazottnak is mondja magát, soha ne töltsön le és telepítsen alkalmazást!**

Az egyik leginkább elterjedt károkozó, „vírusírtónak” is titulált alkalmazás, az Anydesk elnevezést viseli, de vannak más alkalmazások is, amelyek távoli hozzáférést biztosítanak a kiszemelt áldozatok eszközeihez, és az azon tárolt összes fájlhoz, jelszóhoz.

- Ha nem tudja pontosan egy alkalmazásról, mire használható, ne telepítse sem a számítógépére, sem egyéb mobil eszközre, különösen mások kérésére ne tegyen ilyet!
- Ha ilyen, vagy hasonló hívást kap, azonnal ellenőrizze vissza! Hívja fel Ön a számláját kezelő pénzügyintézetet, vagy érdeklődjön személyesen a bankjában!
- Egyeztessen a pénzügyintézettel az Ön számára legideálisabb védelemről!

Ha minden elővigyázatosság, odafigyelés ellenére mégis
bűncselekmény történne a sérelmükre, kérjük azonnal értesítsék a
Rendőrséget!

112