|  |
| --- |
| somogy  cimer  E L B i R  Elektronikus Lakossági Bűnmegelőzési Információs  Rendszer |

Csalók által indított adathalász telefonhívások (vishing) - mi a teendő?

Egyre gyakrabban találkozhatunk kéretlen, gyanús telefonhívásokkal, amikor a csalók bankok vagy cégek nevével visszaélve próbálnak érzékeny pénzügyi adatokat megszerezni ügyfelektől. Az elmúlt időszakban több bank nevében is indítottak adathalász telefonhívásokat gyanús, blokkolt bankkártya tranzakcióra vagy adategyeztetésre hivatkozva.

**Legyen mindig körültekintő kéretlen telefonhívások és SMS-ek esetén!**

* **SOHA NE adja meg a bankkártyája adatait, egyszer használatos SMS-ben kapott vagy online banki jelszavát és PIN-kódját!** A bankok **SOSEM** kérik el ezeket az információkat!
* **Gyanús megkeresés esetén** kérjük, inkább **szakítsa meg** a telefonhívást, majd **hívja** a bank ismert, weboldalán publikált ügyfélszolgálati telefonszámát a hívás valódiságának ellenőrzéséhez!
* **Ne használja** az ellenőrzéshez a hívó által megadott telefonszámot! A szám hamis lehet, vagy kifejezetten a csaláshoz is létrehozhatták!
* **NE hagyja jóvá mobilbanki alkalmazásában az ismeretlen kártyás vásárlásokat, amennyiben azt nem Ön hajtotta végre!**
* **Ne telepítsen ismeretlen eredetű alkalmazást** telefonjára vagy számítógépére, **soha ne engedélyezzen távoli hozzáférést illetéktelen személyeknek eszközéhez!**
* Amennyiben véletlenül kiadta bankkártya vagy egyéb pénzügyi adatait, kérjük, **haladéktalanul hívja** bankja ügyfélszolgálatát.

**További tanácsok az interneten történő biztonságos bankoláshoz**

* **Ne használja az internetbankot e-mailben vagy közösségi médiában kapott linken keresztül**! Az internetbanki felületet mindig a címet kézzel begépelve nyissa meg, még akkor is, ha első látásra megbízható helyről kapta a linket!
* **Figyeljen az úgynevezett adathalász levelekre!** Egyes csalók látszólag a bank nevében küldött e-mailekben kérhetik fel különféle okokkal (fiókfrissítés, fiók tiltás, rendszerkarbantartás, adategyeztetés, stb.) arra, hogy megadja banki adatait egy csaló, a bankéhoz hasonlító weboldalon. **A levelekben közös, hogy minden esetben kérik a csaló weboldal felkeresését, és az adatok megadását.** Mindezt könnyen ellenőrizheti: az egeret a megadott linkre húzva a böngésző megmutatja az oldal címét, így azonnal kiderül, hogy az nem banké. (Figyelmesen nézze meg a hivatkozásokat, néha csak 1-2 betű tér el!) **Soha ne kattintson ilyen oldalakra, és semmiképpen se adja meg adatait! A bankok nem küldenek ilyen típusú e-maileket ügyfeleinek.**
* A fokozott biztonság érdekében az interneten indított banki tranzakciókat (sőt, a netbankba történő belépést is) saját mobileszközön jóvá kell hagyni. Okostelefonját **ne hagyja** védelem nélkül, **használja** a képernyőzárat és a **PIN-kódot** is!
* Amikor új felhasználóként regisztrál a mobiltelefonon működő banki alkalmazásba, különös figyelemmel kezelje a belépéshez szükséges kódokat. A kódot **SOHA ne adja** meg semmilyen böngészőben vagy weboldalon, azt csak a banki mobilalkalmazásban kell beírni. **Ügyeljen rá, hogy ez a kód más kezébe ne kerüljön!**
* Ha bármilyen gyanús körülményt észlel, vagy véletlenül megadata adatait egy csaló weboldalon, **azonnal hívja** bankja központi telefonszámot.

*(Forrás:Raiffeisen Bank)*

**További hasznos információk találhatók az alábbi internetes felületeken:**

http://www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag

<https://nki.gov.hu/>

<https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/>

<https://nki.gov.hu/it-biztonsag/kiadvanyok/szorolapok/>

<https://nki.gov.hu/it-biztonsag/tanacsok/>

https://kiberpajzs.hu/

<https://www.mnb.hu/fogyasztovedelem/hirek-aktualitasok/ne-valjon-szamitogepes-csalas-aldozatava>

<https://www.otpbank.hu/portal/hu/Adathalaszat/kviz>

**NE ADJON ESÉLYT A BŰNÖZÖKNEK!**

**Legyen óvatos!**

**Amennyiben mégis bűncselekmény áldozatává válik értesítse a rendőrséget az ingyenesen hívható 112-es segélyhívó számon!**

****