ELEKTRONIKUS LAKOSSÁGI BŰNMEGELŐZÉSI INFORMÁCIÓS RENDSZER

Lakossági Hírlevél

2023. május

Tegyünk együtt az internetes csalások megelőzése érdekében!

Pénze biztonságban van az illetéktelen hozzáféréstől mindaddig, amíg Ön a személyes és pénzügyi adatait nem teszi hozzáférhetővé illetékteleneknek vagy saját maga nem utalja át a csalóknak.

Legyen nagyon óvatos, ha bank nevében telefonál valaki!

- A beszélgetés elején kérdezze meg, hogy kit keres, és ha nem tudja a pontos nevét, akkor szakítsa meg a hívást!
- Semmilyen programot ne telepítsen, még a bank nevében telefonáló személy kérésére sem!
- Személyes vagy banki adatot, ideértve a bankkártya-adatokat is, ne osszon meg senkivel telefonon, e-mailben! Ha valóban a bank ügyintézője telefonál, ő ismeri a szükséges adatokat!
- Soha ne adja meg netbankja belépési vagy bankkártyája adatait telefonon, e-mailben vagy sms-ben! Ne telepítsen alkalmazást ismeretlen személy kérésére! Ne utaljon biztonsági okból más számlájára! Ezeket banki alkalmazott nem fogja kérni.
- Mindig ellenőrizze a böngésző címsorában, hogy valóban a bank oldalán van-e!
- Mindig ellenőrizze, hogy milyen műveletet (belépést, utalást) hagy jóvá az sms-ben kapott kódjával vagy a mobilbankjával!
- Továbbá mindig legyen körültekintő, ne beszéljen idegenek előtt személyes adatairól, pénzügyeiről, magánéletéről, mert ezeket olyan személyek is hallhatják, akik visszaélhetnek az így megszerzett információkkal!

Ha valamilyen gyanús dolgot tapasztal, hívja fel Ön a bankja ügyfélszolgálatát, így biztos lehet, hogy valóban velük beszél és nem a csalókkal!

Ne feledjék, egy SMS is lehet kártékony!

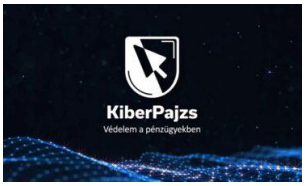
Az elmúlt időszakban több lakossági bejelentés is érkezett a rendőrségre olyan SMS-üzenetekre hivatkozva, amelyben a címzettet egy csomagküldemény rövid időn belüli érkezésére, esetleg megérkezésére emlékeztetik. Az üzenet egy linket is tartalmaz, amelyet megnyitva – a felhasználói bizalom növelése érdekében – ismert csomagküldő szolgálat arculati elmeit is megjelenítik. A gyanútlan felhasználót arra akarják rávenni, hogy a linkre kattintás után telefonjára vagy más okoseszközére egy kártékony alkalmazást telepítsen, amely segítségével az elkövetők hozzáférhetnek az eszközökön tárolt adatokhoz.

A személyes adatok, képek, dokumentumok védelme érdekében az ilyen vagy hasonló SMS üzeneteket érdemes kattintás nélkül törölni.

Az áldozattá válás elkerülése érdekében fogadják meg az alábbi tanácsainkat!

- Ha csomagot rendelt, minden esetben ellenőrizze, hogy valóban attól a csomagküldő-szolgáltatótól kapja-e az értesítést, amelytől a csomagot várja!
- Fontos megemlíteni, hogy a csomagküldő szolgáltatók saját, hivatalos weblapjukra irányítják át a felhasználókat a csomagkövetési rendszer eléréséhez!
- A legtöbb esetben a szolgáltatók közvetlenül az üzenetben is tájékoztatnak a küldemény kézbesítésének várható időpontjáról, azt nem szükséges külön felületen ellenőrizni.
- Az üzenetben érkezett hivatkozásra kattintás előtt minden esetben érdemes megtekinteni, hogy milyen címen nyílik meg az adott tartalom, és amennyiben ez már látszólag is eltér a szolgáltató valós oldalától, azt mielőbb zárja be!
- Soha ne töltsön le vagy telepítsen ismeretlen forrásból származó alkalmazást mobiltelefonjára, okoseszközére!
- Ezen kívül célszerű valamilyen biztonsági szoftver használata is, amely automatikusan blokkolja a kártékony tartalmak elérését.

További hasznos információk:



Bűncselekmény esetén azonnal tegyen bejelentést a legközelebbi rendőrkapitányságon vagy az ingyenesen hívható 112-es segélyhívó számon!