



ELBIR

Elektronikus Lakossági Bűnmegelőzési Információs Rendszer



Legfrissebb kibercsalás típusok



(forrás: internet)

2025 márciusában több kibercsalási módszer is felütötte fejét. Az alábbiakban összefoglaljuk a legfrissebb eseteket és a védekezési javaslatokat:

1. Hamis MNB ügyfél-elégedettségi kérdőívek

A csalók a Magyar Nemzeti Bank (MNB) nevében telefonon keresik meg az ügyfeleket, és ügyfél-elégedettségi felmérésre hivatkozva kérik el bankjuk nevét és e-mail címüket. Ezt követően adathalász e-maileket küldenek, amelyekben kártékony programok letöltésére próbálják rávenni az áldozatokat, vagy telefonon keresztül próbálják megszerezni a banki azonosítókat. Az MNB hangsúlyozza, hogy nem végez ilyen jellegű felméréseket, és felhívja a figyelmet arra, hogy a bankok soha nem kérik el ügyfeleik bizalmas adatait ilyen módon.

Védekezési javaslatok:

- Ne adja meg személyes vagy banki adatait ismeretlen hívások során.
- Ne kattintson ismeretlen forrásból származó e-mailekben található linkekre, és ne töltsön le mellékleteket.
- Ha gyanús megkeresést tapasztal, azonnal lépjen kapcsolatba bankjával.

**Tolna Vármegyei Rendőr-főkapitányság
Bűnmegelőzési Alosztály**

7100 Szekszárd, Mészáros L. u. 19-21.

bunmegelozes.tolnavmrfk@tolna.police.hu

2. Rejtett előfizetések online vásárlások során

Újfajta kibercsalás terjed, amely során a csalók vonzó árú termékeket vagy szolgáltatásokat kínálnak külföldi weboldalakon. A vásárlás során azonban a fogyasztók tudtukon kívül előfizetést is jóváhagynak, ami ismétlődő díjlevonásokhoz vezet.

Védekezési javaslatok:

- Alaposan olvassa el a vásárlási feltételeket, különös tekintettel az apró betűs részekre.
- Kerülje a gyanúsán olcsó ajánlatokat, különösen ismeretlen weboldalakon.
- Rendszeresen ellenőrizze bankszámlakivonatát az ismeretlen tranzakciók kiszűrése érdekében.

3. Signal felhasználókat célzó támadások

Március elején új támadási módszer jelent meg, amely a Signal üzenetküldő alkalmazás felhasználóit célozza. A csalók hamis QR-kódokat használnak arra, hogy hozzáférjenek a felhasználók fiókjaihoz.

Védekezési javaslatok:

- Csak megbízható forrásból származó QR-kódokat olvasson be.
- Legyen óvatos az ismeretlen forrásból érkező üzenetekkel és linkekkel kapcsolatban.

Általános tanácsok a kibercsalások elkerüléséhez:

- Használjon erős, egyedi jelszavakat minden online fiókjához.
- Engedélyezze a kétfaktoros hitelesítést, ahol lehetséges.
- Tartsa naprakészen eszközei szoftvereit és alkalmazásait.
- Legyen szkeptikus a túl jó ajánlatokkal szemben, és mindig ellenőrizze a forrás hitelességét.

Az érintettek áldozatvédelemmel kapcsolatos információkért, bűnmegelőzési tanácsokért fordulhatnak személyesen és telefonon is a Tolna Vármegyei Rendőr- főkapitányság Bűnmegelőzési Alosztály, illetve a városi rendőrkapitányságok munkatársaihoz, illetve írhatnak a kiberkapcsolat@tolna.police.hu e-mail címre is.

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