# Bűnmegelőzési hírlevél
# 2023.július

## Vigyázat, csalók!

Az utóbbi időben nincs olyan nap, hogy ne érkezne feljelentés valamilyen csalásról. Az interneten történő adás-vétel és az ezzel kapcsolatos kisebb-nagyobb visszaélések szinte már meg sem rökönyítik az embert, annál riasztóbb azonban az a tendencia, amelynek során a csalók már nem elégednek meg az egy-egy ügyleten kicsalt pénzzel, hanem mindet akarják, amije csak van a kiszemelt áldozatnak.

Igen gyakori módja a csalásoknak, az úgynevezett „banki csalás", amelyeket rosszindulatú, adathalász telefonhívásokkal valósítanak meg.
**A támadó (a csaló) megpróbálja személyes, pénzügyi vagy biztonsági információi megosztására, vagy pénz átutalására rávenni az áldozatokat.** A telefonáló „ügyintéző" ilyenkor legtöbbször arra hivatkozik, hogy a számlavezető bank egy gyanús tranzakciót észlelt, ezért az ügyfél számláján biztonsági intézkedéseket kell tenni. Ehhez a hívott ügyfélnek állítólag meg kellene adnia internetbankos jelszavát, bankkártyájának adatait vagy egy alkalmazást kellene telepítenie.

- Az ilyen megkeresés esetén szakítsa meg a telefonhívást, majd hívja fel bankjának megbízható ügyfélszolgálati telefonszámát a hívás valódiságának ellenőrzéséhez! A telefonszámról a pénzintézet hivatalos weboldaláról tájékozódhat.
- Legyen gyanús, ha a telefonáló a hívás során számlavezető bankjának megnevezését kéri vagy nem is az Ön bankjától keresi! Más pénzintézet nem tud felvilágosítást adni az Ön tranzakcióiról, illetve nem tudja átkapcsolnia a telefonhívást az Ön bankjához.
- **SOHA NE adja meg a bankkártyája adatait, internetbanki jelszavát, azonosítóját vagy egyszer használatos SMS-ben kapott kódját! A bank ezeket az információkat sosem kéri el.**
- **SOHA NE telepítsen kérésre alkalmazást a telefonjára vagy más digitális eszközeire!** A csalók a legtöbb esetben az AnyDesk vagy TeamViewer nevű szoftverek telepítésére próbálják rávenni az áldozatokat. **Ezek a programok távoli hozzáférést biztosíthatnak az Ön eszközéhez,** a csaló így láthatja, amint belép az internetbanki felületére. Léteznek banki alkalmazások, azonban a pénzintézetek sosem kérik azt, hogy bármilyen alkalmazást telepítsen.
- **SOHA NE utaljon pénzt telefonon érkező kérésre!** Egy bank sosem kér ilyet.

A másik legnépszerűbb módszer napjainkban a Vinted oldal felhasználásával végrehajtott csalás. Hasonlóan működik a „banki csaláshoz", ebben az esetben is cél megszerezni a hozzáférést az áldozat számlájához, ehhez pedig a banki adatai szükségesek. Ehhez első lépésként kicsalják a hirdető e-mail címét, majd erre küldenek e-mailt,benne-egy linket, sokszor a Vinted nevében megerősítendő az eladást vagy vásárlást. A linkre kattintva különböző oldalakon, többnyire ál banki oldalakon, kérik az internet banki adatok megadását is.

- **Ha Ön pénzt vár a számlájára (mert például Ön az eladó), az UTALÓNAK NEM SZÜKSÉGES ISMERNIE AZ ÖN INTERNETBANKOS ADATAIT (felhasználónév, jelszó, egyedi, sms-ben kapott kód, stb). EZEK AZ ADATOK ANNAK NÉLKÜLÖZHETETLENEK, AKI EL AKAR UTALNI AZ ÖN SZÁMLÁJÁRÓL!**

KiberPajzs
Védelem a pénzügyekben

# kiberpajzs.hu

**Tudjon meg többet a kibertérben elkövetett bűncselekményekről!**

**Amennyiben csalás áldozatává válik, minél hamarabb forduljon számlavezető bankjához segítségért és tegyen feljelentést a rendőrségen!**

**Heves Megyei Rendőr-főkapitányság**
**Bűnmegelőzési Alosztály**
**☎:112**

**Segítségért fordulhatnak az áldozatsegítő szolgáltatást nyújtókhoz is:**

**Egri Áldozatsegítő Központ**
**Eger, II. Rákóczi Ferenc utca 10.**
**Tel: +36 (30) 3752176**
**e-mail: askeger@im.gov.hu**

FŐVÁROSI ÉS MEGYEI KORMÁNYHIVATALOKBAN MŰKÖDŐ TERÜLETI ÁLDOZATSEGÍTŐ SZOLGÁLATOK:

ÁLDOZATSEGÍTŐ KÖZPONTOK:

WWW.VANSEGITSEG.HU

IGAZSÁGÜGYI MINISZTÉRIUM

ÁSK
ÁLDOZATSEGÍTŐ KÖZPONT

KORMÁNYHIVATALOK