



**Amennyiben telefonon vagy üzenetben,  
e-mailben keresnek soha**

**SENKINEK NEM ADOM MEG**

**SZEMÉLYES ADATAIMAT**

**A BANKKÁRTYÁM SZÁMÁT**

**PIN KÓDOMAT**

**CVC KÓDOMAT**

**INTERNETES BELÉPÉSI ADATAIMAT**

**MERT EZ**



- **Internetbankolásra a bank applikációját használom;**
- **Gyanakszom, ha váratlan felszólítást kapok pl. streaming szolgáltató vagy hatóság nevében;**
- **Ha pénzt várok, nem adom meg a pénz küldőjének a bankkártya adataimat;**
- **Mielőtt egy webcímre látogatok a webcím melletti lakat ikonra kattintva ellenőrzöm, hogy biztonságos-e az oldal;**
- **Gyanúsnak ítélem meg a magyartalan kifejezéseket egy szövegben, felszólításban;**
- **Soha nem kattintok csatolmányokra, linkekre megszokásból, mindig körültekintően járok el.**

**ÖN IS TUD VÉDEKEZNI AZ INTERNETES CSALÁSOK ELLEN! LÁTOGASSON  
EL A [WWW.KIBERPAJZS.HU](http://WWW.KIBERPAJZS.HU) WEBOLDALRA ÉS TÁJÉKOZÓDJON!**





## **Vigyázzon vásárláskor! Az internetes csalások már az online piactéren, apróhirdetési oldalakon is megjelentek!**

Az utóbbi hónapokban jelentősen emelkedett az online csalások száma. Az elkövetők minden esetben pénzt akarnak kicsalni a kiszemelt áldozatoktól, akik semmit nem sejtenek arról, hogy csalóval állnak szemben és saját maguk adják ki személyes-, illetve bankkártya adataikat.

Az online piactéren, apróhirdetési oldalakon / Vinted, Jófogás, Marketplace / elkövetett csalások többsége az alábbi módon történik:

Az eladó (a későbbi sértett) eladásra kínál egy ( bármilyen ) terméket, melyre vevőként jelentkeznek be az elkövetők. A potenciális vásárló elkéri az eladó email címét, melyre elküld egy emailt, mintha az oldal küldte volna és egy kitöltendő online űrlapot küld, ahol az eladónak meg kell adnia a személyes- és bankkártya adatait.

Előfordulhat, hogy az e-mail címre egy weboldal linkjét küldik, mely szintén adathalász oldal. A tapasztalatlan eladók kiadva saját adataikat azonnal bűncselekmény áldozatává válnak, miután az elkövetők pénzt emelnek le bankszámlájukról.

## **Összeszedtük, milyen esetben kell gyanakodnunk, hogy csalóval van dolgunk!**

- A vásárlónak semmi oka arra, hogy elkérje az Ön e-mail címét, telefonszámát vagy bankkártyaszámát, ezért ezeket soha ne adja ki!
- Lehetőleg semmilyen linkre ne kattintson rá, amit üzenetben küldenek!
- Ha már megadta valakinek az adatait a platformon és kap egy első pillantásra valódinak tűnő e-mailt, gondolkodjon el! Van-e az üzenetnek

**PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG  
BŰNMEGELŐZÉSI OSZTÁLY**



**ELBIR**  
Elektronikus Lakossági Bűnmegelőzési Információs Rendszer



értelme, magyarul írták-e, nyelvtanilag helyes-e? Mindenképp ellenőrizze, hogy milyen email címről küldték, ha pedig elbizonytalanodik, lépjen kapcsolatba az ügyfélszolgálattal az oldalon és inkább győződjön meg róla, hogy az email valóban tőlük származik! (Ezt más csalásokra is érdemes alkalmazni: ha a bank küld valamilyen figyelmeztető emailt, járjon utána, valós-e!)

- Ha az üzenetben néhány órás határidőt szabnak, az már egy figyelmeztető jel. Sem az online piacterek, sem a bankok nem fognak csupán 1-2 órát adni a fizetésre és teljesen értelmetlen is lenne ennyire siettetni az ügyfelet a kártyaadatok megadásával.
- Mindig nézze meg, hogy a tényleges weboldalon van-e vagy ahova átkattint valóban az online piactérhez tartozik! Bármilyen írásjel, más domain a cím végén, vagy egy olvashatatlan URL olyan weboldalra irányíthat, ahol már csalásnak van kitéve.

### **Legyen óvatos, ne váljon csalás áldozatává!**

Ha mégis megtörténne, tegyen feljelentést a rendőrségen! A 112-es segélyhívó szám ingyenesen hívható. A <http://www.police.hu/ugyintezes/beadvanytetel> oldalon minden szükséges információt megtalál.

**PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG  
BŰNMEGELŐZÉSI OSZTÁLY**

1145 Budapest, Róna utca 124. ☒: 1557 Budapest, Pf. 20. ☎: 460-7101; BM: 28-811  
E-mail: [elbir@pest.police.hu](mailto:elbir@pest.police.hu)



**ELBIR**  
Elektronikus Lakossági Bűnmegelőzési Információs Rendszer



## **Hívja az „Igazságügyi Rendőrséget” – új módszerekkel próbálkoznak a csalók, az Interpol és a rendőrség nevében küldenek leveleket.**

Valótlan tartalmú levelek terjednek az interneten, amelynek aláírójaként rendőri vezetőket jelölnek meg. Legyen körültekintő az érkező e-mailekkel és ne adjon esélyt a csalóknak! Ha a rendőrség vagy az Interpol nevében kap gyanús levelet, hagyja figyelmen kívül!

### **Az alábbi árulkodó jelek utalhatnak arra, hogy az emailt csalók küldték:**

- Nemzeti Rendőrség Főigazgatóság nem létezik, Országos Rendőr-főkapitányság a helyes megnevezés;
- Igazságügyi Rendőrség szintén nem létezik;
- Interpol Központi Iroda (ICB) nem létezik;
- A nyelvtanilag helytelen megfogalmazás ugyancsak csalókra utalhat;
- Amennyiben Magyarország Rendőrsége e-mailben kommunikál, azt nem külföldi email címről teszi,
- Az Országos Rendőr-főkapitányság se az Interpol, se az Europol nevében nem kommunikál, azt csak saját nevében, saját email címéről teszi,
- A törvényi hivatkozások pontatlan megjelölése (pl: a Büntetőeljárás törvénykönyv 390-1. cikke nem létezik. Helyesen 2017. évi XC. törvény a büntetőeljárásról. A 390. szakasz nem arról szól, amire a levél utal, és nincs külön cikke sem).

**PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG  
BŰNMEGELŐZÉSI OSZTÁLY**

1145 Budapest, Róna utca 124. ☒: 1557 Budapest, Pf. 20. ☎: 460-7101; BM: 28-811

E-mail: [elbir@pest.police.hu](mailto:elbir@pest.police.hu)





**ELBIR**  
Elektronikus Lakossági Bűnmegelőzési Információs Rendszer



**Így néznek ki a hamis, csaló levelek:**



**A NEMZETI RENDŐRSÉG FŐIGAZGATÓSÁGA  
INTERPOL KÖZPONTI IRODA – EUROPOL**



**Bírósági vizsgálati jelentés (a büntetőeljárás törvénykönyv 390-1. cikke)**

... vezetője az Interpol Központi Irodával (ICB) együttműködve.

Ezt az e-mailt egy internetes nyomozás keretében küldjük Önnek (ez az intézkedés az interneten keresztül elkövetett bűncselekmények ellenőrzésére jogosult), hogy tájékoztassuk Önt arról, hogy Ön több bűncselekmény tárgyát képezi, mint például

- GYERMEKPORNOGRÁFIA
- HONLAP-PORNOGRÁFIA
- CYBERPORNOGRÁFIA
- SZEKUALIS BÜNCSELEKMÉNYEK

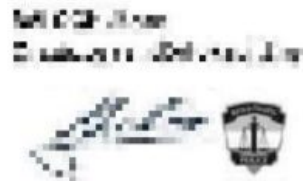
Ezeket a bűncselekményeket a számítógépes rendőrség az Ön IP-címéről rögzítette. Tájékoztatásul közöljük, hogy a 2007. márciusi 390-1. számú nemzetközi büntető törvénykönyv az interneten elkövetett szexuális támadást vagy szexuális erotikát bünteti.

**Kérjük, válaszoljon e-mailben részletes magyarázattal 72 órán belül.**

Amennyiben Öntől nem kapunk választ, kötelesek leszünk továbbítani feljelentésünket Dr. POLT Péter legfőbb ügyésznek, hogy szerezzen elfogatóparancsot az Ön letartóztatására, és haladéktalanul intézkedjen az Ön letartóztatásáról.

Önt mint szexuális bűnözőt nyilvántartásba vesszük. A fényképét és a vádirat összes bizonyítékát elküldjük a médiának sugárzásra, hogy családjá és barátai megtudják, mit csinál a számítógép előtt.

Ezennel figyelmeztetjük



**PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG  
BŰNMEGELŐZÉSI OSZTÁLY**

1145 Budapest, Róna utca 124. ☒: 1557 Budapest, Pf. 20. ☎: 460-7101; BM: 28-811  
E-mail: [elbir@pest.police.hu](mailto:elbir@pest.police.hu)



**ELBIR**  
Elektronikus Lakossági Bűnmegelőzési Információs Rendszer



----- Forwarded message -----  
Feladó: Rendőrség Police <pj.interpls@outlook.es>  
Date: 2023. febr. 25., Szo 17:13  
Subject: Jó reggelt kívánok  
To:

## **HÍVJA AZ IGAZSÁGÜGYI RENDŐRSÉGET**

Bírósági vizsgálat céljából (az eljárási törvénykönyv 390-1. cikke)

figyelmedbe

Az Europol Hivatal a nemzeti bűnüldöző hatóságokkal együttműködve  
Lépjen kapcsolatba vele röviddel a számítógépes támadás után a számítógépes beszivárgás miatt  
(Engedélyezett, különösen a gyermekpornográfia területén,  
Pornóoldal, Internetes pornó,  
kiállítás, amely tudatja Önnel, hogy Ön a téma  
Néhány hatályos jogi eljárás:

GYERMEKPORNOGRÁFIA  
PORNOGRÁF OLDAL  
KIBERPORNOGRÁF  
KIÁLLÍTÁS

Kérjük, azonnal válaszoljon nekünk e-mailben.  
Ez szigorúan 12 órán belül megtörténik.  
Ezt követően kénytelenek vagyunk elküldeni  
jelentésünket d.r Varga Judit igazságügy-miniszternek  
kiadja az elfogatóparancsot  
és azonnal letartóztatták és felvették a szexuális bűnelkövetők nemzeti nyilvántartásába.



Minden elektronikus levél feladóját ellenőrizze! Soha ne kattintson megszokásból és mindig legyen körültekintő! Amennyiben egy levelet gyanúsnak ítél, ne teljesítse a kért adatszolgáltatást!

**PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG  
BŰNMEGELŐZÉSI OSZTÁLY**

1145 Budapest, Róna utca 124. ☒: 1557 Budapest, Pf. 20. ☎: 460-7101; BM: 28-811

E-mail: [elbir@pest.police.hu](mailto:elbir@pest.police.hu)



**ELBIR**  
Elektronikus Lakossági Bűnmegelőzési Információs Rendszer



## NE VÁLJON ÁLDOZATTÁ! VÉDEKEZZEN AZ INTERNETES CSALÁSOK ELLEN!

**LAJOS**

- AZ OVIBAN IS CSAVARKULOS VOLT A JELE
- AZ EGÉSZ UTCA TŐLE KÉR SZERSZÁMOKAT

**ÁTLÁT A HAMIS BANKI HÍVÁSOKON**

**A CSALÓK GYAKRAN ADJÁK KI MAGUKAT BANKI DOLGOZÓNAK ÉS SÜRGETŐ ÜGYEKKEL PRÓBÁLNAK ÁTVERNI.**

TE IS TUDSZ VÉDEKEZNI AZ INTERNETES CSALÁSOK ELLEN. LÁTOGASS EL A [WWW.KIBERPAJZS.HU](http://WWW.KIBERPAJZS.HU) WEBOLDALRA!

**KiberPajzs**  
Védelem a pénzügyekben

Tájékozódjon a [www.kiberpajzs.hu](http://www.kiberpajzs.hu) weboldalon!



**PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG  
BŰNMEGELŐZÉSI OSZTÁLY**

1145 Budapest, Róna utca 124. ☒: 1557 Budapest, Pf. 20. ☎: 460-7101; BM: 28-811  
E-mail: [elbir@pest.police.hu](mailto:elbir@pest.police.hu)



## Internet tudatosan – online is biztonságban

A közelgő nyári vakáció idején is fontos hogy figyeljünk az online tér biztonságára. Kérjük, hogy olvassák el a figyelemfelhívó sorokat és beszéljenek gyermekeikkel arról, hogy az Interneten nem mindenki az, akinek mondja és mutatja magát.



### BARÁT VAGY VESZÉLY?



Az interneten szerezhetsz új ismerősöket, de találkozhatasz rossz emberekkel is. Olyannal, aki csak kihasználni akar. Eleinte kedves veled, hogy a bizalmadba férközzön. Pedig lehet, hogy nem is az, akinek mondja magát. Például nem gyerek, hanem felnőtt. Akit nem ismersz személyesen, az IDEGEN, és légy vele nagyon ÓVATOS!

### ISMERD FEL A VESZÉLYT!



Ha valaki, akivel online beszélsz, csetelsz:  
- izgatón/erotikusan megérinti magát előtted,  
- azt kéri, hogy te érintsd meg izgatón/erotikusan magad előtted,  
- erotikus képeket vagy videókat mutat neked,  
- intim képet kér rólad,  
- olyat tesz vagy mond, amitől kellemetlenül érzed magad!

### AMIT TEHETSZ!



ÁLLÍTSD BE,  
hogy személyes adataidat, képeidet csak ismerőseid láthassák a közösségi oldalakon!  
KAPCSOLD BE  
a felhasználói fiókok védelme érdekében a kétfaktoros hitelesítést!  
SZÓLJ SZÜLEIDNEK,  
ha beszélgetés során kellemetlenül vagy veszélyben érzed magad, fenyegetnek vagy zsarolnak!

### AMIT NE TEGYÉL!



NE OSSZ MEG  
magadról intim vagy kínos helyzetben készült képet!  
NE ADJ KI  
magadról személyes információkat (pl.: iskola neve, lakcím, pontos születési dátum, telefonszám) ismeretlennek!  
NE BÍZZ  
olyanban, akit személyesen nem ismersz!

További aktuális tartalmakért ( tanácsokért, felhívásokért) kövessék az Internet tudatosan – online is biztonságban Facebook oldalt, amelyet az alábbi hivatkozáson érnek el:

<https://www.facebook.com/internettudatosan>



## Internet tudatosan – online is biztonságban

### Kétfaktoros hitelesítés

#### 1. Mi az a kétfaktoros hitelesítés?

A hagyományos felhasználói név és jelszó páros mellett a felhasználói fiókba (pl. Facebook, Gmail, Instagram, netbank, online tárhely, stb.) történő belépéshez még egy másik módon is hitelesíteni kell a felhasználót, vagyis nem elég a jelszó ismerete.

#### 2. Miért fontos a kétfaktoros hitelesítés használata?

A felhasználói név/jelszó páros manapság már nem nyújt elég erős védelmet a felhasználói fiókoknak. A jelszavak kiszivároghatnak, kitalálhatóak, feltör-hetőek és birtokukban az arra nem jogosult személyek is beléphetnek a felhasználói fiókba. A kétfaktoros hitelesítés alkalmazásával ezt tudjuk megelőzni.



#### 3. Hogyan történik a kétfaktoros hitelesítés?

A második hitelesítési lépésként jellemzően egy egyszerhasználatos kód (One Time Password) megadásával történik. Ez a kód érkezik egy korábban megadott e-mail címre, illetve mobiltelefonszámra SMS-ben.

Másik lehetőség, hogy egy mobiltelefonos alkalmazásban generált, az adott felhasználói fiókhoz tartozó 6 számjegyű kódot kell megadni. Ez a kód 30 másodpercenként változik, és mindig csak az aktuálissal lehet belépni a felhasználói fiókba. Ez megoldás biztonságosabb, mint az e-mail-es vagy SMS-es kódküldés.

Netbankba vagy a Google fiókba történő belépést a bank, illetve a Google saját mobiltelefonos alkalmazásában lehet jóváhagyni. Erre egy felugró üzenetben figyelmeztet az alkalmazás. A netbankok esetében általában alapértelmezetten be van állítva a kétfaktoros hitelesítés. Itt is érdemes azonban a hitelesítés módjaként a bank saját mobiltelefonos alkalmazását választani a SMS vagy email helyett.

#### 5. Kétfaktoros hitelesítő (Two-factor authentication - 2FA) alkalmazás beszerzése és használata

A 2FA alkalmazást androidos telefonra Google Play Áruházból vagy iOS készülékre az App Store-ból tudunk letölteni. Ingyenes megoldásként ajánljuk a 2FA Authenticator alkalmazás használatát. Az alkalmazásban tárolt adatok PIN kóddal, illetve ujjlenyomattal védhetőek és beállítható, hogy a Google Drivera vagy iCloudba készítsen biztonsági mentést róluk. Így a mobiltelefon elvesztése vagy meghibásodása esetén is visszaállíthatók egy új készüléken. Új QR kód beolvasása + gombra kattintva történik.

#### 6. Hogyan lehet bekapcsolni?

A kétfaktoros hitelesítést érdemes minden esetben a számítógép böngészőjében bekapcsolni. A beállításához szükség lesz egy androidos mobiltelefonra vagy iPhone-ra.

#### Facebook

Lépj be a Facebook fiókodba!

A kétfaktoros hitelesítést az alábbi menüben lehet bekapcsolni:

Fiók – Beállítások és adatvédelem – Beállítások – Biztonság és bejelentkezés – Kétfaktoros hitelesítés használata – Módosítás – Hitelesítő alkalmazás használata

1. A rendszer kéri a fiók használatának megerősítését.
2. Beállítás külső hitelesítő alkalmazáson keresztül
3. QR kód beolvasása az alkalmazással (pl. 2FA Auth)
4. Kattints a Folytatás gombra
5. Megerősítő kód beírása
6. Visszaigazolás

#### Google

Lépj be a Gmailbe!

Kattints a jobb felső sarokban profilképre – Google fiók kezelése – Biztonság – Bejelentkezés a Google-ba – Kétfaktoros azonosítás – Bejelentkezés telefon segítségével

1. Kattints a Beállítás gombra!
2. Jelszó újbóli megadása.
3. Telefon kiválasztása és kattints a Tovább gombra!
4. Próbá következ. Kattints a Tovább gombra!
5. Véglegesítés! Kattints a Bekapcsolás gombra!

További aktuális tartalmakért ( tanácsokért, felhívásokért) kövessék az Internet tudatosan – online is biztonságban Facebook oldalt, amelyet az alábbi hivatkozáson érnek el:

<https://www.facebook.com/internettudatosan>

**Pest Vármegyei Rendőr-főkapitányság  
Bűnmegelőzési Osztály**

**PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG  
BŰNMEGELŐZÉSI OSZTÁLY**

1145 Budapest, Róna utca 124. ☒: 1557 Budapest, Pf. 20. ☎: 460-7101; BM: 28-811

E-mail: [elbir@pest.police.hu](mailto:elbir@pest.police.hu)





## Internet tudatosan – online is biztonságban

### Router

A routerünk az otthoni hálózatunk bejárati ajtaja, a jelszó pedig a kulcs hozzá. A gyári jelszó nem biztonságos, ezért azt mindenképpen érdemes megváltoztatni! Ebben segítünk most.

**Mi az a router?**

A router az otthoni hálózat és az internet összekapcsolását és az adatforgalmat irányító eszköz. Sok esetben az internetszolgáltató biztosítja a felhasználóknak a routert, ehhez csatlakoznak vezetékkel vagy vezeték nélkül (WIFI-n) keresztül az eszközeink. Használhatunk saját routert is, ilyenkor ezt a szolgáltató eszközehez kell csatlakoztatni, és az internetszolgáltató eszköze csak átjáróként funkcionál. Ebben az esetben a saját routerünk általában több funkcióval rendelkezik.

**Hogyan változtassuk meg a router gyári jelszavát?**

Mind szolgáltatói, mind a saját router adminisztrációs felületét a böngészőben lehet elérni, a router IP címének megadásával. Ez gyártóként változik, de általában 192.168.0.1. vagy 192.168.1.1, és a router alján lévő címkén vagy a csomagolásán szerepel. Az IP címet a böngészőbe bírva megjelenik bejelentkezési felület, ahol meg kell adni az adminisztrátori jelszót, és egyes típusoknál a felhasználói nevet. A gyári jelszó és a felhasználói név is „admin”, de ez is megtalálható a router alján lévő címkén és felhasználói útmutatóban.

A felhasználói routereknél a bekapcsolást követő első beállításkor általában kéri ennek megváltoztatását. Minden esetben egyedi, másol nem használt jelszót adjunk meg, amit jegyezzünk fel egy papírra, és tegyünk biztonságos helyre.

Akkor is változtassuk meg saját routerünk jelszavát – és ha lehet, a bejelentkezéshez szükséges felhasználói nevet is –, ha ezt a beállításkor nem ajánlotta fel. Hasonlóan járjunk el a szolgáltatói router esetében is. A szolgáltató által végzett frissítéskor az alapértelmezett adatokra visszaállíthatja ezeket a beállításokat).

A felhasználói nevet általában az Adminisztráció vagy Rendszer menüpontban lehet megváltoztatni. Ehhez meg kell adni a régi jelszót, majd általában kétszer az újat.

**Miért kell megváltoztatni a router gyári jelszavát?**

A router adminisztrációs felületére történő belépéshez jelszóra van szükség. Ez minden eszköz esetében gyárilag megegyezik, általában „admin”. A jelszó birtokában illetéktelenek is hozzáférhetnek a routerhez, módosíthatják a beállításait és elérhetik az otthoni hálózatot, valamint a rajta található eszközöket is. A routerünk az otthoni hálózatunk bejárati ajtaja, a jelszó pedig a kulcs hozzá. Csak akkor ér valamit, ha egyedi és csak mi ismerjük azt.

További aktuális tartalmakért ( tanácsokért, felhívásokért) kövessék az Internet tudatosan – online is biztonságban Facebook oldalt, amelyet az alábbi hivatkozáson érnek el:

<https://www.facebook.com/internettudatosan>

**Pest Vármegyei Rendőr-főkapitányság  
Bűnmegelőzési Osztály**

**PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG  
BŰNMEGELŐZÉSI OSZTÁLY**

1145 Budapest, Róna utca 124. ☒: 1557 Budapest, Pf. 20. ☎: 460-7101; BM: 28-811

E-mail: [elbir@pest.police.hu](mailto:elbir@pest.police.hu)





## Internet tudatosan – online is biztonságban



„Ma reggel a +36 1 636 6666 számról hívott az OTP Bank nevében telefonáló egyik – férfi – csaló. Mivel a beszélgetés nagyon tanulságos volt, megosztjuk annak legfontosabb tapasztalatait.

A csaló azért hívott, mert a bankkártyámmal gyanús online tranzakciót akartak végrehajtani az Alza webáruházában. A telefonhívás alatt próbált nagyon profinak tűnni, de érződött rajta, hogy nem igazi ügyfélszolgálatos. A beszélgetés közben sokszor megakadt, bizonytalan volt. A technikai, jogi, szakmai kifejezéseket rosszul használta. Ez persze nem mindenkinek tűnik fel, számomra azonban kifejezetten szórakoztató volt. Hangsúlyozta, hogy semmilyen személyes adatot nem kér, bele tudna nézni a banki anyagomba de az engedélyem nélkül nem teszi, ezzel is próbálta elnyerni a bizalmamat. Mivel mindenben nagyon együttműködőnek mutatkoztam és a feltett kérdésekre válaszoltam, javasolta, hogy egy alkalmazást telepítsek az eszközöm, hogy azzal tudjam elvégezni a kétfaktoros hitelesítést, amivel fokozhatom a biztonságot. Ez egy távoli asztal elérést biztosító program lett volna, amivel hozzáfértek volna minden, a készüléken tárolt információhoz. Ezt a kérését természetesen már nem teljesítettem.

Kis internetes kutatás alapján látjuk, hogy a napokban több sikertelen próbálkozása is volt csalónknak. Az interneten az alábbi véleményeket írták erről a telefonszámról érkezett hívásokkal kapcsolatban:

- OTP ügyfél szolgálatosnak adta ki magát egy hölgy és azt állította, hogy fizetni próbáltak a kártyámmal az Alzánál... Mivel nem vagyok az OTP ügyfele, így hamar véget ért a beszélgetés
- Ma hívott, hogy pénzt akartak leemelni a számlámról, de beszélni sem tud!
- OTP-s csalás, applikáció telepítésre akartak rávenni
- Szerencsétlen csaló, két mondatot nem tud összerakni.
  - ✓ Legyünk nagyon óvatosak, ha bank nevében telefonál valaki!
  - ✓ A beszélgetés elején kérdezzük meg, hogy kit keres, és ha nem tudja a pontos nevünket, akkor szakítsuk meg a hívást!
  - ✓ Semmilyen programot ne telepítsünk, még a bank nevében telefonáló személy kérésére sem!
  - ✓ Személyes vagy banki adatot, ideértve a bankkártya-adatokat is, ne osszunk meg senkivel telefonon! Ha valóban a bank ügyintézője telefonál, ő ismeri a szükséges adatokat!”

További aktuális tartalmakért ( tanácsokért, felhívásokért) kövessék az Internet tudatosan – online is biztonságban Facebook oldalt, amelyet az alábbi hivatkozáson érnek el:

<https://www.facebook.com/internettudatosan>



## Internet tudatosan – online is biztonságban

### Veszélyes melléletek!

Fertőzött Word vagy Excel fájlok érkezhettek e-mail melléleteként. Úgy tűnik, mintha az e-mail egy korábbi levelünkre érkezett volna válaszként.

A fájlok megnyitása után az alkalmazás kéri, hogy engedélyezzük a tartalmat vagy a makrók futtatását. Amennyiben ez megtörténik, egy kártékony kód települhet a számítógépünkre, ami ellophatja személyes és banki adatainkat vagy SPAM-ek küldésére használhatja számítógépünket.

#### ! Tanácsok:

⚠ Ne nyisson meg gyanús hivatkozásokat vagy melléleteket!

✓ Ellenőrizze, hogy a MS Word, MS Excel, MS PowerPoint makróbeállításai megfelelőek-e:

Fájl – Beállítások – Adatvédelmi központ – Az Adatvédelmi központ beállításai – Makróbeállítások:  
Az összes makró letiltása értesítéssel.

✗ Fájl megnyitáskor ne kattintson a Tartalom engedélyezésére vagy a Makrók futtatására addig, amíg a fájl küldőjével nem egyeztetett, arról hogy valóban szükséges-e engedélyezni!



További aktuális tartalmakért ( tanácsokért, felhívásokért) kövessék az Internet tudatosan – online is biztonságban Facebook oldalt, amelyet az alábbi hivatkozáson érnek el:

<https://www.facebook.com/internettudatosan>

**Pest Vármegyei Rendőr-főkapitányság  
Bűnmegelőzési Osztály**

**PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG  
BŰNMEGELŐZÉSI OSZTÁLY**



**ELBIR**  
Elektronikus Lakossági Bűnmegelőzési Információs Rendszer



## NE VÁLJON ÁLDOZATTÁ! VÉDEKEZZEN AZ INTERNETES CSALÁSOK ELLEN!

**ANNA**

- MINDENKI SZÜLETÉSNAPOJÁT FEJBŐL TUDJA
- MINDIG AD BORRAVALÓT A FUTÁROKNAK

**ÁTLÁT A CSALÓK SMS-ÜZENETEIN**

**A CSALÓK ARRÁ ALAPOZNAK, HOGY MINDEN LINKET ÉS CSATOLMÁNYT KÉRDÉS NÉLKÜL MEGNYITUNK.**

TE IS TUDSZ VÉDEKEZNI AZ INTERNETES CSALÁSOK ELLEN.  
LÁTOGASS EL A [WWW.KIBERPAJZS.HU](http://WWW.KIBERPAJZS.HU) WEBOLDALRA!

**KiberPajzs**  
Védelem a pénzügyekben

Tájékozódjon a [www.kiberpajzs.hu](http://www.kiberpajzs.hu) weboldalon!



**PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG  
BŰNMEGELŐZÉSI OSZTÁLY**

1145 Budapest, Róna utca 124. ☒: 1557 Budapest, Pf. 20. ☎: 460-7101; BM: 28-811  
E-mail: [elbir@pest.police.hu](mailto:elbir@pest.police.hu)



**ELBIR**  
Elektronikus Lakossági Bűnmegelőzési Információs Rendszer



## RAVASZ MINT A ...

### ADATHALÁSZ ÜZENETEK A FOXPOST NEVÉBEN

Az elmúlt hónapokban valótlan tartalmú, a FOXPOST nevében küldött adathalász/csaló e-mailekkel és üzenetekkel, illetve telefonon keresztül próbálkoznak a csalók, a felhasználók banki adatait megszerezni.

Az adathalász üzeneteket a legtöbb esetben ismert cégek nevében küldik a támadók. Nehéz ezeket megkülönböztetni a hiteles, valós üzenetektől, mivel céges logókat és grafikus elemeket, adatokat használ(hat)nak.

Az adathalász e-mailek gyakran részletekbe menően hasonlítanak a valódiakra, az ezekben található rosszindulatú hivatkozásokat úgy tervezik meg, mintha a cég valós weboldalára irányítana át. Azonban a linkek olyan oldalakra vezethetnek, ahol a csalók meg tudják szerezni lakossági felhasználók és üzleti partnereik adatait, amelyekkel később visszaélhetnek.

#### Hogyan ismerhetők fel az adathalász e-mailek vagy más üzenetek?

→ a levélben szereplő **link helytelen pl.: foxpost-hu.kaspay24.hu**

→ az üzenetben lévő **adatok nem pontosak, vagy helyesírási hibákat, hibás nyelvezetet** tartalmaznak, illetve **magyartalan, online programmal fordított mondatok** találhatóak benne

→ **direkt fizetési hivatkozás** szerepel benne pl.: <https://foxpost-hu.hufpay.site/18981955>

#### Ha szokatlan és gyanús linkkel találkozik, ne kattintson rá!

Ha arra gyanakszik, hogy adathalász-támadás célpontjává vált, kérjük, **az ilyen jellegű leveleket hagyja figyelmen kívül és semmiképpen se kattintson** a “FOXPOST nevében” küldött e-mailben lévő **gyanús, helytelen linkre**, mert ezek nem a FoxPost Zrt. által küldött hivatalos értesítők.

#### Amennyiben telefonon keresztül próbálják megszerezni az adatait, semmiképp ne adja ki azokat!

A FOXPOST soha nem kér banki belépési adatokat sem telefonon, sem más formában. Továbbá **nem kezdeményez olyan telefonhívást, amelyben a szállítás megerősítésére buzdítana**. Amennyiben ilyen jellegű hívást kap, azonnal szakítsa meg.

### Vigyázzanak az online térben is értékeikre!

PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG  
BŰNMEGELŐZÉSI OSZTÁLY

1145 Budapest, Róna utca 124. ☒: 1557 Budapest, Pf. 20. ☎: 460-7101; BM: 28-811

E-mail: [elbir@pest.police.hu](mailto:elbir@pest.police.hu)





## Veszélyes Netflix-lehúzás terjed!

Továbbra is terjednek az SMS-csalások, a technológia fejlődésével és terjedésével újabb és újabb módszert találnak ki a csalók. A furcsa központosással írt szöveg szerint a Netflix-előfizetésünkkel van probléma, egészen pontosan "utolsó figyelmeztetés a fiókjának korlátozása előtt", szöveggel. Az SMS olyan mobilszámról érkezik, amelyet már számos alkalommal jelentettek különböző telefonszámokat listázó oldalakon a felhasználók "veszélyes" számként. Ezért érdemes résen lenni, az üzenetet azonnal törölni!

A kétes eredetű linkre kattintva egy adatahalász oldal nyílik meg, ahol bankkártyaadatainkat szeretnék a csalók megszerezni.

A közeli hozzátartozókat, rokonokat és ismerősöket is figyelmeztesse, hogy semmiképp ne kattintsanak az említett linkre, **azonnal töröljék az ilyen üzeneteket!**





**ELBIR**  
Elektronikus Lakossági Bűnmegelőzési Információs Rendszer



**+33628736342** 1



Ez az üzenet egy nem mentett számról érkezett.  
Óvakodjon az SMS-ben és más módon történő  
adathalásztól.

**Szám blokkolása**

december 24., szombat

Netflix : Legutobbi befizetését  
elutasítottak,kérjük, er sitse  
meg fizetési adatait, különben  
fiokjat felfüggesztjük:  
[netflix.korlátozás.com](https://netflix.korlátozás.com)

21:51

**PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG**  
**BŰNMEGELŐZÉSI OSZTÁLY**

1145 Budapest, Róna utca 124. ✉: 1557 Budapest, Pf. 20. ☎: 460-7101; BM: 28-811

E-mail: [elbir@pest.police.hu](mailto:elbir@pest.police.hu)





## HÍVÓSZÁM SPOOFING: HÍVÓSZÁM-HAMISÍTÁS!



A hívószám **spoofing**, azaz hívószám-hamisítás a vishing (hamis banki hívások) adathalász tevékenységek egyik speciális elkövetési technikája. Lényege, hogy az elkövetők módosítják a hívószámot, ami a hívott fél telefonjának kijelzőjén megjelenik, ezzel elrejtve a valódi hívó fél azonosságát. Vagyis híváskor nem a hívást kezdeményező

igazi telefonszáma jelenik meg a potenciális áldozatok készülékén, hanem egy másik, jellemzően olyan, ami ismerős: például egy banké, ezáltal még inkább hitelesnek beállítva a hívást. Az ilyen hívások célja elsősorban a bizalom kiépítése, illetve az adathalász támadások elszámú védvonalának, az óvatosságnak a kiiktatása: ha az áldozat ismerős telefonszámot lát, amikor hívják, kevésbé lesz gyanakvó és megnő az esélye annak, hogy teljesíti, amit a hívó fél kér tőle.

### Mit tegyen?

- Kezelje óvatosan, fenntartással a kéretlen telefonhívásokat!
- Minél sürgetőbb a hívás és az üzenet, annál gyanúsabb! Lassítson és gondolja át alaposan, hogy mit is kérnek valójában!
- Gyanús telefonhívás esetén ne adjon meg személyes adatokat és szakítsa meg a beszélgetést!
- Ha a kijelzett telefonszám valóban a bank ügyfélszolgálati telefonszáma, az sem garancia arra, hogy tényleg onnan keresik. Annak ellenőrzésére, hogy az illető valóban az, akinek mondja magát, keresse meg a szervezet telefonszámát és lépjen vele kapcsolatba közvetlenül! Fontos, hogy az ügyfélszolgálat felé a kapcsolatfelvételt, hívást Ön kezdeményezze az ismert telefonszámon, ne hagyatkozzon visszahívásra vagy átkapcsolásra, amit a csalók felajánlanak.
- Az ellenőrzéshez ne használja a hívó által megadott telefonszámot! A szám hamis lehet vagy létrehozhatták kifejezetten a csaláshoz.
- A csalók az interneten könnyen megszerezhetik az alapvető információkat Önről, például a közösségimédia-profilok felhasználásával. Nem bízhat meg a hívóban csak azért, mert ő ismeri ezeket az adatokat.
- Ha hitelesnek gondolja a telefonhívást, akkor is kérjen keresztazonosítást, melynek során a feltett kérdésekre (például anyja születési neve) a válaszok egyik felét az intézmény ügyintézője adja meg, a válaszok másik felét pedig Ön!

PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG  
BŰNMEGELŐZÉSI OSZTÁLY



**ELBIR**  
Elektronikus Lakossági Bűnmegelőzési Információs Rendszer



- Soha ne adja meg a betéti vagy hitelkártyája PIN-kódját, CVV-kódját, online banki jelszavát vagy az egyszer használható, második hitelesítési kódot! A bankok, banki ügyintézők sosem kérik el ezeket az információkat!
- Soha ne telepítsen mások kérésére olyan programot számítógépére vagy telefonjára, amit nem ismer! A csalók sokszor vírusvédelmi megoldásnak vagy szoftverfrissítésnek beállítva, álcázva próbálják rávenni áldozatukat arra, hogy visszaéléshez használható programot telepítsenek.
- Soha ne utaljon pénzt telefonon érkező kérésre! Egyik bank sem kér ilyet.
- A csalási szándékú hívásokat jelentse a bankjának!

**Pest Vármegyei Rendőr-főkapitányság**

**PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG  
BŰNMEGELŐZÉSI OSZTÁLY**

1145 Budapest, Róna utca 124. ✉: 1557 Budapest, Pf. 20. ☎: 460-7101; BM: 28-811  
E-mail: [elbir@pest.police.hu](mailto:elbir@pest.police.hu) KÉR azonosító: ORFK PEST