

# ELBIR

Elektronikus Lakossági Bűnmegelőzési Információs Rendszer



Veszprém  
Vármegyei

Rendőr-főkapitányság

2023.  
MÁRCIUS



## KÜLÖNSZÁM

Nem tudtuk kézbesíteni a csomagját, az újrakezesítéshez látogasson el erre a linkre: <https://deilverminute.com/r/twFprDJ>

Tisztelt ügyfelünk,

A csomagot megkapta az Ön számára 113704981 az alábbi címen  
Cím: 80529 HUF  
Dátum: 16/03/2023.  
Rövid a csomagról

**CSOMAG VÁRAKOZIK**  
Csomag száma: #HUN98465ZPOSTA

Utolsó alkalommal értesítettük a kézbesítésre váró szállítási költség kapcsán.  
Ha az összeg néma kifizetve 48 órán belül, a fűgőben lévő kézbesítés történik lez.

Csomag adatai Állapot:  
Állapot: A csomag a Zóna Terminál várakozik  
Csomag:  
Kézbesítési idő: [ ] munkanap

**KiberPajzs**

Szokatlan tevékenységet észleltünk fiókjában. Az oldalad korlátozott, ami azt jelenti, hogy a fiókod által kezelt oldal adatai a közösségi szabványait. Az Ön védelme érdekében oldaladat nem mindenki láthatja a és nem használhatod a fiókod által kezelt oldalat.  
Az alábbi linke kattintva igazolnunk kell személyazonosságát:  
• <http://myipari.com/9991632626>  
Közösségi alapelveink segítenek megérteni a biztonságát.  
Ne felejtse, hogy 24 óra van ezen lépések végrehajtására, hogy megakadályozza fiókja végleges leállítását.  
Üdvözléssel,  
Security Group.

A megadott címre nem tudtuk kiszállítani a csomagot. Kerjen második kísérletet a következő link segítségével <https://expresscardparcel.com/r/lpi1UM>

[ ]  
Utolsó figyelmeztetés a fiókjának korlátozása előtt, kérjük, erősítse meg adatait 24 órán belül : <korlatozas-.x.com>

Te vagy a videóban? 🤖  
📺  
<http://tiktok.r317j.cloud/ZTV5Ebc>

Kuldeménykísérlet 2/2 - 36203305754 - az On #IPS208497103HU csomagja, vissza lesz kuldvé 14-10-2022, ha nem erősíti meg: <efuvul.link/4DVAsbZ>

+48  
On fizetni próbált 50,000HUF értékben, ha mégsem on volt kattintson ide: <https://hu-.com/login>

Vegyen részt a felmérésben és nyerjen 100 000 Ft-ot  
Csak felhívó ügyfelek számára

Uj csomagok az oldaladon  
Hozza létre a csomagját és kövesse a szállítást

# NE DÖLJÖN BE!

[www.kiberpajzs.hu](http://www.kiberpajzs.hu)

# FŐKAPITÁNY AJÁNLÁSÁVAL

Kedves Olvasó!

Tisztelettel ajánlom a Veszprém Vármegyei Rendőr-főkapitányság 2023. március havi bűnmegelőzési hírlevelének különszámát.

Külo nszámunkban felhívjuk a figyelmet az online csalásokra és kérjük, **NE DŐLJENEK BE!** A saját biztonságuk érdekében fogadják meg a külö nszámunkban közzétett ORFK tájékoztatójában foglalt tanácsokat, ajánlásokat az online csalások visszaszorítására.

Dékány Balázs r. ezredes  
rendőrségi tanácsos  
rendőrfőkapitány

## Összefogás az online csalások visszaszorítása érdekében

Napjainkban egyre gyakrabban találkozunk az online térben elkövetett csalási módszerekkel, ezért az ilyen típusú bűncselekmények visszaszorítása érdekében [KiberPajzs](#) néven közös oktatási és kommunikációs együttműködésről döntött a Magyar Nemzeti Bank, a Magyar Bankszövetség, a Nemzeti Média- és Hírközlési Hatóság, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet és az Országos Rendőr-főkapitányság. A programról az alapítók még 2022. november 7-én beszámoltak.

A tapasztalat azt mutatja, hogy minden törekvés ellenére növekszik az interneten elkövetett csalások száma, és a módszerek is változnak. Annak érdekében, hogy a digitális térben se váljanak áldozattá az emberek, az ORFK, a Magyar Bankszövetség és a NBSZ Nemzeti Kibervédelmi Intézet 2023. március 7-én közös sajtótájékoztatón számolt be az újabb típusú online csalásokról és az áldozattá válás megelőzésének lehetőségeiről.

Oláh-Paulon László r. alezredes, az ORFK Bűnmegelőzési Osztály vezetője elmondta, az elmúlt egy évben közel háromszorosára növekedtek az online térben elkövetett bűncselekményeknek a számai. Ki lehet jelteni, hogy legjobb módja az áldozattá válás elkerülésének, ha megismerjük a legújabb és legelterjedtebb elkövetési módokat. Felismerjük azokat a jeleket, amik utalhatnak a rosszindulatú elkövetőkre. Ezeket megismerve nem dőlünk be ezeknek a trükköknek. A [KiberPajzs](#) programnak azért lett alapítótagja a rendőrség, mert a rendőrség egyik fő feladata a bűnmegelőzés.

A közoktatási intézményekben folytatott rendőrség biztonságra nevelő programjainak egyik meghatározó alapelemévé vált az online biztonság oktatása. De nem csak iskolákban, hanem közösségi média felületeken illetve a rendőrség saját online felületén is rendszeres figyelemfelhívó közleményeket teszünk közzé. Ilyenek voltak a közelmúltban rendőri vezetők nevével visszaélve megküldött adathalász e-mailek, valamint online kereskedelmi oldalon regisztrált eladók tudatos megtévesztése témakörben kiadott közlemények.

Sütő Ágnes a Magyar Bankszövetség főtitkár-helyettese kitért arra, hogy 2023. március 6-10. között zajlik a PÉNZ7 program az iskolákban, több mint 1000 iskola közel 140 ezer diákja részvételével. Az idei pénzügyi téma a „Korszerű pénzkezelés és digitális biztonság”, ami lehetővé teszi, hogy általános- és középiskolai tanórákon önkéntes szakértők bevonásával tanuljanak a diákok pénzügyi digitális alapismereteket. A Magyar Bankszövetség Digitális Szimat Kihívást hirdetett, amelyben életkortól függetlenül tehetjük próbára tesztkérdésekkel a digitális biztonsági felkészültségünket, és kipróbálhatjuk „Okosabbak vagyunk-e mint egy hacker?”.

A programban egy ismert gamer és egy etikus hacker együtt segítik a felkészülést.

Simon Edina nb. százados, az NBSZ NKI szóvivője felhívta a figyelmet arra, hogy az adathalász-támadás, bármilyen csatornán is érkezen, valójában egyfajta pszichológiai hadviselés az online térben. A felhasználó megtévesztésével a kiberbűnözők megpróbálják rávenni az áldozatot arra, hogy személyes adatokat, érzékeny információkat adjon át számukra, vagy egy vírussal megfertőzzék a számítógépét. Amíg azonban a korábbi években a támadások kevésbé előkészítettek voltak, és jobban magukon hordozták a felismerhető jeleket, amellyel a szemfülesek át tudtak látni rajtuk, addig napjainkban a támadások komplexek és sokkal inkább célzottak, jobban kihasználják a napi aktualitások okozta realitás erejét (legyen szó akár egy bank technikai leállásáról, vagy egy online streaming szolgáltatás által bejelentett felhasználói feltétel változásáról). A naprakész tartalmú támadással pedig hihetőbb keretet adnak a csalásnak.

A veszély forrása, az ilyen jellegű támadások közös pontja, pedig a szöveges üzenetben található link. A link, amelyre kattintva vagy egy adatlap, regisztrációs felület található (ahol a megtévesztett áldozat önként megadja a bizalmas adatait), vagy egy kártékony tartalom lakozik.

A sajtótájékoztatón a szakemberek ismertették az új elkövetési módszert. „Smishing” (az angol „SMS” és „phishing”, vagyis SMS és adathalász szavak kombinációja) olyan csalás, amelynél a támadó SMS segítségével próbál megszerezni személyes, pénzügyi vagy biztonsági információkat. Jellemzően egy beágyazott link van az egyébként szokványosnak tűnő üzenetben (pl. csomagod érkezett). A küldő megbízható forrásnak álcázza magát, úgy tesz, mintha egy bank, kártyakibocsátó, futárszolgálat, közműszolgáltató vagy valamilyen egyéb szolgáltató képviselőjében jelentkezne. Az üzenet arra kéri a címzettet – általában sürgető módon –, hogy nyisson meg egy weboldalra vezető hivatkozást, telepítsen egy alkalmazást, vagy hívjon fel egy telefonszámot a fiókja ellenőrzése, frissítése vagy újraaktiválása érdekében. A hivatkozás hamis weboldalra mutat, a telefonszámon pedig egy csaló jelentkezik, aki az adott cég munkatársának adja ki magát. Célja olyan információk megszerzése, amelyek segítségével aztán ellophatják az áldozat pénzét.

# ÍGY PRÓBÁLJÁK MEG BECSAPNI AZ ONLINE TÉRBEN (Fals e-mailek, SMS-ek, levelek)

Nem tudtuk kézbesíteni a csomagját, az újrakezesítéshez látogasson el erre a linkre:  
<https://deilverminute.com/r/twFprDI>

Tisztelt Ügyfelünk,

A [REDACTED] információ, hogy az Ön szállása 9757445HU, és díjforrása [REDACTED]

Díjak: 805,28 HUF

Dátum: 16/01/2023.

Küldje el a csomagomat

**CSOMAG VÁRAKOZIK**

Csomag száma:  
#HUN984652POSTA

Utolsó alkalommal emlékeztetjük a kifizetésre váró szállítási költség kapcsán.

Ha az összeg nincs kifizetve 48 órán belül, a függőben levő kézbesítés törölve lesz.

**Csomag adatai Állapot:**

Állapot: A csomag a 2-es Terminál várakozik

Csomag: [REDACTED]

Kézbesítési idő: (2) munkanapon belül

Követ



Szoktalan tevékenységet észleltünk fiókjában. Az oldalad korlátozott, ami azt jelenti, hogy a fiókad által kezelt oldal sérti a közösségi szabványait. Az Ön védelme érdekében oldaladat nem mindenki láthatja a [REDACTED], és nem használhatod a fiókad által kezelt oldalt.

Az alábbi linkre kattintva igazolnunk kell személyazonosságát:

• <http://tinyurl.com/9981632626>

Közösségi alapelveink segítenek megőrizni a biztonságát.

Ne feledd, hogy 24 órája van ezen lépések végrehajtására, hogy megakadályozza fiókja végleges letiltását.

Üdvözlettel,  
Security Group.

A megadott címre nem tudtuk kiszállítani a csomagot. Kerjen második kísérletet a következő link segítségével <https://expresscardparcel.com/r/pli1UM>

[REDACTED] Utolsó figyelmeztetés a fiókjának korlátozása előtt, kérjük, erősítse meg adatait 24 órán belül: [korlatozas-...x.com](https://korlatozas-...x.com)

Te vagy a videóban? 🤖  
🤖  
<http://tiktok.r317j.cloud/ZTV5Ebc>

Küldeménykísérlet 2/2 - 36203305754 - az On #IPS208497103HU csomagja, vissza lesz küldve 14-10-2022, ha nem érositi meg: [efuvul.link/4DVAsbZ](http://efuvul.link/4DVAsbZ)

Vegyen részt a felmérésben és nyerjen 100 000 Ft-ot  
Csak felöltött ügyfelek számára

[Kérdés? Nézze meg a kérdéseket](#)

© 2022 [REDACTED] Minden jog fenntartva. További információk

+48  
On fizetni próbált 50,000HUF értékben, ha mégsem on volt kattintson ide: <https://hu-...com/login>

**HÍVJA AZ IGAZSÁGÜGYI RENDŐRSÉGET**

Bűnügyi elnökség felhívja az igazságszolgáltatás 390-1. cikkéről

figyelmeibe

Ismeri a nemzeti bűnügyi hatóságokkal együttműködésbe való (vagyis) a szándékosan tervezett és szándékosan beszervezés miatt azt, különösen a gyermekpornográfia területek, internetes pornó, mely katalógus Önmel, hogy Ön a vélem helyre jog eljárás:

GYERMEKPORNOGRÁFIA  
PORNOGRÁF OLDAL  
KIBERPORNOGRÁF KÁLLITÁS

személy választjon helyre e-mailben, csak 12 óra belül megválaszolni.  
Ön kénytelenek vagyunk elküldeni meg a Varga Judit igazságügy-miniszternek elfogadhatatlanságát a bűnözés és a szexuális bűnözésről nemzeti nyilatkozatára.

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

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

Dr. [REDACTED] 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
- SZEXUÁLIS BŰNCSELEKMÉNYEK

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 médianak sugárzásra, hogy családja és barátai megtudják, mit csinál a számítógép előtt.

Ezennel figyelmeztetjük

2023. január 16. 10:00



# NÉHÁNY JÓ TANÁCS, hogyan ne váljon online csalók áldozatává

1. Gondolja át a kapott üzenet tartalmát. Tisztázza magában, hogy a leírtak mennyire felelhetnek meg a valóságnak. Lehet, hogy az adott szolgáltatásnak vagy banknak nem is az ügyfele? Egy olyan szolgáltatástól kap sms-t, ahol korábban nem adta meg a telefonszámát? Nem is rendelt semmit, mégis hogyan érkezhetne csomagja?
2. Amennyiben nem tudja eldönteni egy üzenet valóságtartalmát, vegye fel a kapcsolatot a küldővel. Keresse fel például a szolgáltatója, a bankja vagy a hivatkozott csomagküldő szolgálat hivatalos honlapját, esetleg hívja fel őket a hivatalos telefonszámukon. Amennyiben egy közösségi oldalon privát üzenetet kap egy ismerlentől? Hagyja figyelmen kívül. Azonban ha egy ismerőstől, kérdezzen vissza a linkre kattintás előtt, mit küldött Önnek az illető.
3. Mindig legyen gyanakvó a mások által kezdeményezett olyan kapcsolatfelvétellel szemben, amikor nem tud minden kétséget kizáróan megbizonyosodni a másik fél kilétéről. Ne adja meg illetékteleneknek személyes, pénzügyi és biztonsági adatait! Ha egy gyanús üzenet egy linket vagy egy mellékletet tartalmaz, ne kattintson rá és ne is töltsse le.
4. Az esetek túlnyomó többségében az online térben működő bűnözők az emberi kíváncsiságot használják ki. Ne dőljön be egy ismeretlen feladótól kapott üzenetnek, ne akarjon csak most az egyszer kattintani, még akkor sem, ha az üzenet szerint egy videót talált Önről egy ismerőse. Egy nem várt és minden előzmény nélkül kapott linket vagy csatolmányt ne nyisson meg.
5. Amennyiben adathalász-támadás célpontjává vált, jelezze ismerőseinek, ezzel segítve az ő online biztonságukat. Nem volt elég szemfüles egy adathalász-üzenet kapcsán, és rákattintott az abban található linkre? Haladéktalanul vegye fel a kapcsolatot a számlavezető bankjával, és tegyen feljelentést a rendőrségen!
6. Ne kattintson kéréstlen szöveges üzenetekben érkezett hivatkozásokra, mellékletekre vagy képekre a küldő személyazonosságának ellenőrzése nélkül! Az ellenőrzéshez keressen rá a számra az interneten (ha csalásról van szó, valószínűleg nem Ön lesz az első), vagy hasonlítsa össze a számot az érintett szervezet hivatalos telefonszámával!
7. Azonnal vegye fel a kapcsolatot a bankjával, ha azt gyanítja, hogy egy smishing üzenetre válaszolt és megadta banki adatait!

**Forrás:** <https://www.police.hu/hu/hirek-es-informaciok/bunmegelozes/aktualis/ne-doljon-be-0#2>

Hozzájárulásunkat adjuk ahhoz, hogy Kedves Olvasóink a Hírlevél tartalmát részben vagy egészben szabadon felhasználják, a célszervezetek felé eljuttassák.

Kérjük azonban, hogy a terjesztés során hivatkozzanak arra, hogy a Hírlevelet a Veszprém Vármegyei Rendőr-főkapitányság Bűnmegelőzési Osztálya készítette.

## IMPRESSZUM

Kiadja: a Veszprém Vármegyei Rendőr-főkapitányság

Bűnügyi Igazgatóság Bűnmegelőzési Osztálya

Telefon / fax: 06-88/ 544-683

E-mail: [futtaton@veszprem.police.hu](mailto:futtaton@veszprem.police.hu)

