



ELBIR
Elektronikus Lakossági Bűnmegelőzési Információs Rendszer

NE DŐLJÖN BE!

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 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 sajtótájékoztatót számolt be az újabb típusú online csalásokról és az áldozattá válás megelőzésének lehetőségeiről.

A sajtótájékoztatón a szakemberek ismertették az új elkövetési módszert. „Smishing” (az angol „SMS” és „phishing”, vagyis SMS és adathalászat 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 weboldatra 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 kezbesíteni a csomagját, az újrakezesítéshez látogasson el erre a linkre:
<https://deilverminute.com/r/twFprDI>

Tisztelt Ügyfelünk,

A csomagja, hogy az Ön számlájára 975744381, az előfizetése vár.

Díjak: 805,28 HUF

Dátum: 16/01/2022.

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 Terminálban várakozik

Csomag:

Kézbesítési idő: (2) munkanapon belül

Követ



Szokatlan tevékenységet észleltünk fiókjában. Az oldalad korlátozott, ami azt jelenti, hogy a fiókod által kezelt oldal sérti a közösségi szabványait. Az Ön védelme érdekében oldaladat nem mindenki láthatja a közösségi oldalon, és nem használhatod a fiókod által kezelt oldalt.

Az alábbi linke kattintva igazolnunk kell személyazonosságát:

• <http://tinyurl.com/9981632626>

Közösségi alapelveink segítenek megőrizni a biztonságát.

Ne feledje, hogy 24 órája 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/lpltiUM>

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

Te vagy a videóban? 🤖

<http://tiktok.r317j.cloud/ZTV5Ebc>

Kuldemenykísérlet 2/2 - 36203305754 - az On [#IPS208497103HU](https://208497103HU) csomagja, vissza lesz küldve 14-10-2022, ha nem erósi meg: efuvul.link/4DVA5bZ

Vegyen részt a felmérésben és nyerjen 100 000 Ft-ot

Csak felidőre ügyfelek számára

[Kérdés / Válasz](#)

100 000 Ft-ot nyerhetnek
100 000 Ft-ot nyerhetnek
100 000 Ft-ot nyerhetnek

További információk

+48

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

----- Folyóirat megérkező -----
 Köszönjük a megrendelést
 Szám: 2022. máj. 25. - 10.11.23
 Számla: 10.11.23

HÍVJA AZ IGAZSÁGÜGYI RENDŐRSÉGET

Bűnügyi vizsgálat céljából (az eljárás törvénykönyve 290-1. cikke)

figyelmeztető

Az Európai Hivatal a nemzeti bűnüldöző hatóságokkal együttműködve
 Legyen kapcsolatba vele röviddel a számítógépes támadás után a számítógépes bűncselekmény miatt
 (Engedélyezett, különösen a gyermekpornográfia területén,
 Pornográfia, internetes pont,
 kártevő, amely tudatja Önnek, hogy Ön a téma
 Néhány hatóság jogi eljárás:

GYERMEKPORNOGRÁFIA
 PORNOGRÁF OLDAL
 KIBERPORNOGRÁF
 KÁRTÉVŐ

Kérjük, azonnal válaszoljon nekünk e-mailben.
 Ez szigorúan 12 órán belül meg kell történnie.
 Ezt követően kiegészítendő vagyunk elküldeni
 jelentésünket a d. Varga József igazságügyi miniszternek
 kádjá az elfogadottan
 és azonnal lezárunk és felvesszük a szexuális bűncselekmények nemzeti nyilvántartásába.



A NEMZETI RENDŐRSÉG FŐIGAZGATÓSÁGA
 INTERPOL KÖZPONTI IRODA – EUROPOL



Bűnügyi vizsgálati jelentés (a bűntörvénykönyv 390-1. cikke)

Az Európai Hivatal a nemzeti bűnüldöző hatóságokkal együttműködve (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
- SEXUÁLIS BŰNCSELEKMÉNYEK

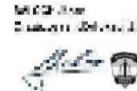
Ezeket a bűncselekményeket a számítógépes rendőrség az Ön IP-címéről rögzítette.
 Tájékoztatásul közöljük, hogy a 2007. márciusi 390-1. számú nemzetközi büntető törvénykönyv az interneten elkövetett szexuális támadást vagy szexuális erotikát bünteti.

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, mi csinál a számítógép előtt.

Ezennel figyelmeztetjük



Néhány jó tanács, hogy ne váljon online csalók áldozatává:

Gondolja át a kapott üzenet tartalmát. Tisztázza magában, hogy a leírtak mennyire feleltethetőek 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?

1. 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 ismeretlentől? Hagyja figyelmen kívül. Azonban ha egy ismerőstől, kérdezzen vissza a linkre kattintás előtt, mit küldött Önnek az illető.
2. 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.
3. 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.
4. 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!
5. Ne kattintson kéretlen 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!
6. Azonnal vegye fel a kapcsolatot a bankjával, ha azt gyanítja, hogy egy smishing üzenetre válaszolt és megadta banki adatait!

www.kiberpajzs.hu

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