



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 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 TÉRBE (Fals e-mailek, SMS-ek, levelek)

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

Üdvözlő Ügyfélnk,
 Név: [REDACTED]
 Email: [REDACTED]

CSOMAG VÁRÁROZDI
 Csomag címe: **HERNIAOSZPONTA**

Utolsó alkalommal érkeztetjük a kifizetése más szállítási költség kiegészítéssel.

Ha az összeg nincs kifizetve 48 órán belül, a csomagot levél kiküldésére kerülhet.

Csomag adatai Állapot:
 Állapot: A csomag a 2. sz. Társaságunkhoz került
 Csomag: [REDACTED]
 Kiszámlázott idő: [REDACTED]

Küld

Szociális tevékenységek elvégzése. Az oldalról kiderült, hogy az újrakezesítéshez látogasson el erre a linkre:
<https://deilverminute.com/r/twFprDj>

A megadott címre nem tudtuk kiszállítani a csomagot. Kerjen második kísérletet a következő link segítségével <https://expresscardparcel.com/r/lp1tUM>

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 érosíti meg: efuvul.link/4DVAsbZ

Utolsó figyelmeztetés a fiókjának korlátozása előtt, kérjük, erősítse meg adatait 24 órán belül : korlatolasa-.../x.com

+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 feladat megoldása után


HÍVJA AZ IGAZSÁGÜGYI RENDŐRSÉGET

Kérjük figyeljen a közértesítőjére 2022. 10. 14. napján

Figyelmeztetés

Az Országos Rendőrfőkapitányság felhívja a figyelmét, hogy a közértesítőjében szereplő információk nem minősülnek jogi tanácsnak, és nem kötelezők a megvalósításra. A közértesítőjében szereplő információk nem minősülnek jogi tanácsnak, és nem kötelezők a megvalósításra.

Országos Rendőrfőkapitányság
 FŐKAPITÁNYSÁG
 KÖZÉRTESETŐ



A NEMZETI RENDŐRSÉG FŐIGAZGATÓSÁGA
 INTERPOL KÖZPONTI IRODA – EUROPOL

INTERNET



Figyelmeztetés

Az Országos Rendőrfőkapitányság felhívja a figyelmét, hogy a közértesítőjében szereplő információk nem minősülnek jogi tanácsnak, és nem kötelezők a megvalósításra.

Figyelmeztetés

Az Országos Rendőrfőkapitányság felhívja a figyelmét, hogy a közértesítőjében szereplő információk nem minősülnek jogi tanácsnak, és nem kötelezők a megvalósításra.

Figyelmeztetés

Az Országos Rendőrfőkapitányság felhívja a figyelmét, hogy a közértesítőjében szereplő információk nem minősülnek jogi tanácsnak, és nem kötelezők a megvalósításra.

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>