TÉMA

Online csalások
(Természetes- és Mesterséges intelligencia által)

Falussy Péter
Joós Attila
WWW.WEBMARK.HU

„Ha 1x átversz az a te szégyened, ha 2x akkor az az enyém…”

webmarkeurope
www.webmark-europe.com

Miért Csalnak Online a Csalók? Mert megtehetik!

MIÉRT?

1. Anyagi Haszonszerzés - Pénzért
Cél: Pénzszerzés áldozatoktól különböző módszerekkel (pl. adathalászat, hamis weboldalak).
Kockázat: Nagy anyagi veszteségek a cégek számára.

2. Személyes Adatok Megszerzése - Adatokért (majd eztán Pénzért)
Cél: Érzékeny információk (bankkártya adatok, jelszavak) megszerzése és felhasználása.
Kockázat: Adatvédelmi incidensek, reputációs kár.

3. Identitáslopás - Rejtettségért - Anonimitásért (másodlagosan a többi okból)
Cél: Mások nevében csalások végrehajtása, hitelfelvétel.
Kockázat: Jogilag és pénzügyileg is terhelheti a vállalkozásokat.

4. Manipuláció és Hatalomgyakorlás - Hatalomért
Cél: Áldozatok manipulálása, pszichológiai befolyásolás.
Kockázat: Ügyfélbizalom csökkenése, brand erózió

5. Könnyű Célpontok - Gyakorlásért /Izgalomért / Pénzért
Cél: Nagy számú potenciális áldozat elérése alacsony kockázattal.
Kockázat: Fokozott kitettség a vállalkozások számára.

6. Alacsony Kockázat - Gyakorlásért / Izgalomért /Pénzért
Cél: Anonim tevékenység az online térben, nehéz nyomozhatóság.
Kockázat: Jogérvényesítés nehézségei, fokozott veszély.

Konklúzió: A csalók fő motivációi az anyagi haszon, az adatok megszerzése és a manipuláció. Vállalkozóként kiemelten fontos az online biztonságra és a kockázatkezelésre fókuszálni.

Veszélyben vannak-e a gyerekek? *Igenis + Nemis*

SAFE

TOP csalások az elmúlt időszakból (MOL-os)

TOP

Scholarship centrally
Hirdetés

Egy hónappal ezelőtt 80 000 **Ft** fektettem be a **MOL** új projektjébe, és már meg is kaptam az első csekket.

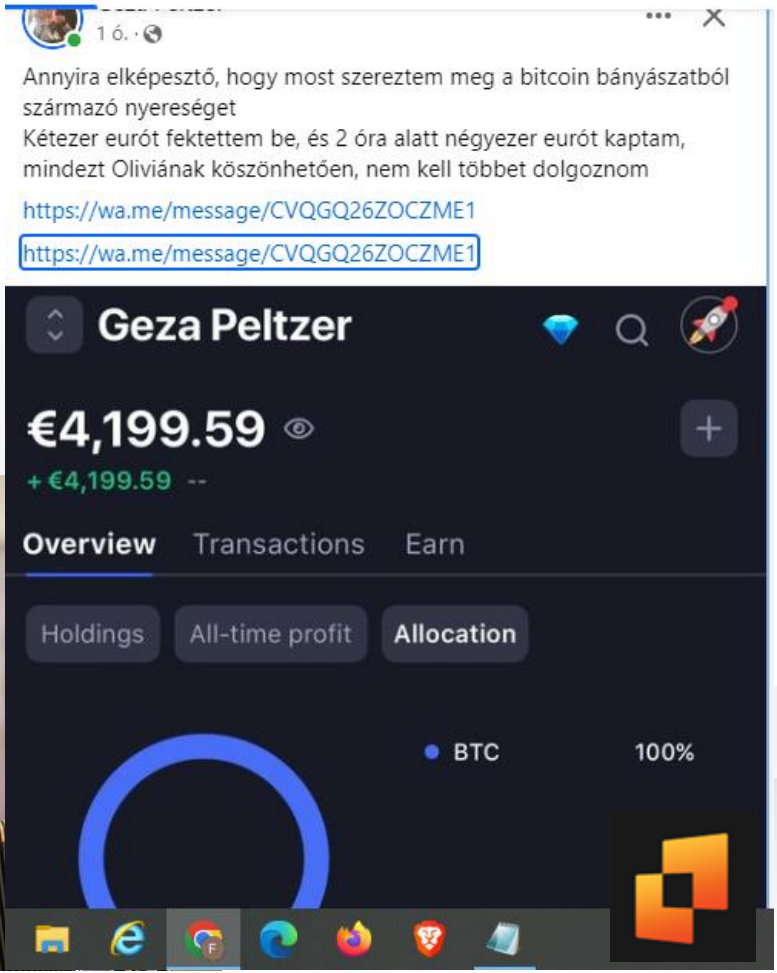
Mindenkinek ajánlom! Jelentkezzen, és egy menedzser visszahívja, és elmondja, hogyan kezdje el. Csak 15-20 pe szabadidőre van szükséged.

TOP csalások az elmúlt időszakból (MOL-os)

TOP

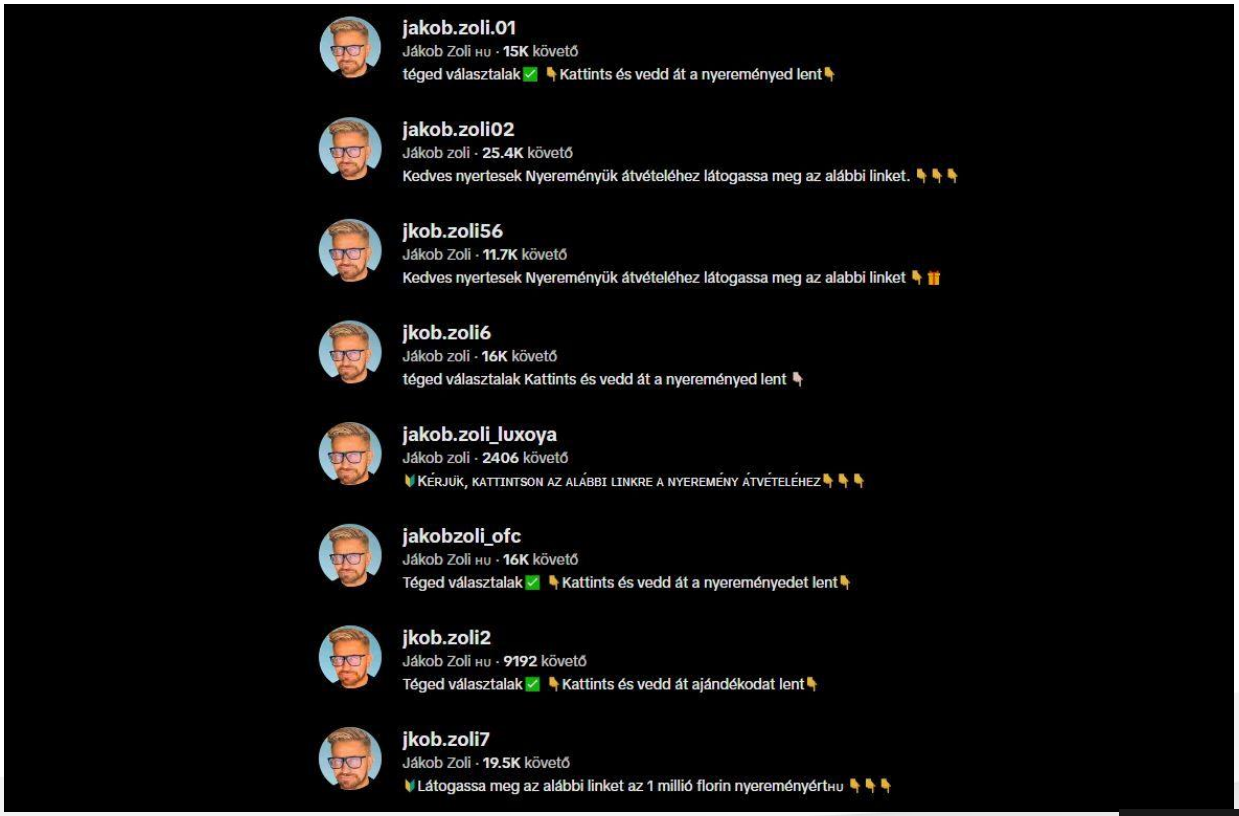
TOP csalások az elmúlt időszakból (Bitcoin)

TOP



TOP csalások az elmúlt időszakból (Jákob Zoli)

TOP



TOP csalások az elmúlt időszakból (Repteres)

TOP

Budapest Liszt Ferenc Nemzetközi Repülőtér
Hirdetés ·

A reptéren kirakjuk a raktárt és eladjuk az elveszett poggyászokat 729 Ft-ért! Minden bőrönd tele van különféle dolgokkal és elektronikával 📦. 🚚 Kiszállítás az ország egész területén. Az ajánlat csak a hónap vé géig érvényes online. 60 nap a visszatérítésért 📅. A megrendeléshez k attintson a hirdetésben található gombra és menjen az oldalra! 👇
https://air3panda6.store/products/cases-of-unclaimed-and-lost-airport-luggage?utm_campaign=eVCsQxC7sR&fbclid=

Budapest Liszt Ferenc Nemzetközi

TOP csalások az elmúlt időszakból (Repteres)

TOP

Budapest Liszt Ferenc Nemzetközi Repülőtér bejegyzése

Jázmin Patakiné
Ti vagytok a legjobbak, köszönöm szépen! Találtam benne készpénzt és a bőrönd is jó. Nyaralást tervezek 🥰. Ha valaki még kételkedik, ajánlom ezt az akciót!

1 n. Tetszik Válasz 5

Jázmin Kissné
Megdöbbentett a sokféle dolog a bőröndben, amit kaptam. Találtam egy hatalmas mennyiségű márkás ruhát, egy Macbookot, de zárva, valamint Ray-Ban napszemüveget, és volt készpénz a pénztárcában🤩

Mekkora kárt okoznak? Mik a trendek?

TRENDS

- A csalók minden **10 percben valakinél** próbálkoznak!
- **Naponta kb. 60 millió Ft a lopás** (47 család megtakarítását jelenti - 700 ezer Ft/alkalom - 15x lett a sikeres támadások száma 3 éves viszonylat https://nepszava.hu/3246568_megtakaitas-csalasok-47-csalad-naponta
- **Top csalás - AI csalás 9 millliárd Ft -os HongKong** - deepfake (erőforrás és tudás igényes) Minden érintettel egyeztetett online, csak ők deepfake eszközökkel voltak hamisítva https://hvg.hu/tudomany/20240205_deepfake_penzugyi_vezeto_atveres_videohivas
- **Booking csalás - trendi és szezonális** - itt egy nyaralás ára a bukás! “Hiba a tranzakciónál kérem fizesse be újra” - érzelmi nyomás https://index.hu/gazdasag/2024/08/13/booking-com-szallas-foglalas-mesterseges-intelligencia-ai-chatgpt-kiberbunozes-csalok/
- **Decatlon csalás - “megszólalásig hasonló”** weboldalak Lemásolják a jó márka ismertségü oldalakat és elterelik a vásárlókat https://hvg.hu/tudomany/20231124_decathlon_csalas_atveres_hamis_weboldal_ezekre_kell_figyelni_megtevesztes_tranzakcio_penz_megszerzese

Érzelmek az értelem felett?!

webmarkeurope
www.webmark-europe.com

Mit tudunk tenni?

VÉDELEM

- “Csak egy kattintásra vagyunk a csalóktól” - minden kattintás előtt legyél tudatos - a link szövegét alaposan olvasd el!

- Inkább kérdezz meg egy szakembert

- Munkahelyen extra óvatosan - legyén inkább te a “buta kérdező”, mint a kárt okozó szereplő

- Levelező programok tanítása - AI bejön, de nem “szentírás” a döntése!

- Weboldalak amikről vásárolsz, ott a kártyás fizetéssel óvatosan!

- Biztonságos eszközök telefon és gép (gyakran átnézetni)

- Kis pénzösszeget tartalmazó kártyák használata (külön kártya/számla)

- Biztonságos applikációk használata (feleslegesek törlése)

Ne kapkodj - Kérdezz szakembert!

Ki a cégünknél/családban a leggyengébb láncszem?

???

Oktatás és képzés fontosságát nem lehet eléggé kiemelni!

Mit tudunk tenni még?

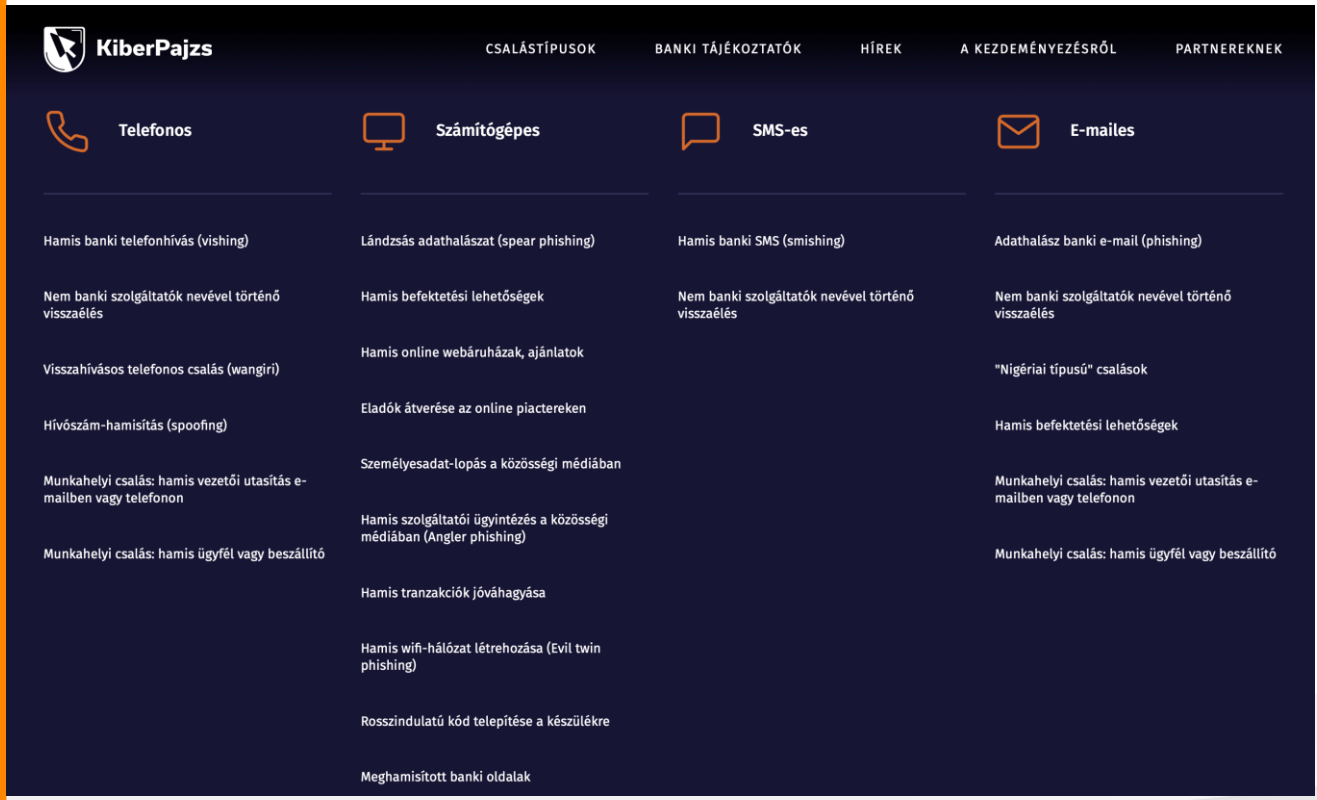
PAJZS

Hivatalos kibervédelmi portál
- friss hírekkel és oktató célzattal
https://kiberpajzs.hu/

A félelem információ szerzéssel csökkenthető

Csalási formák csatornánként

FORMÁI



https://kiberpajzs.hu/csalastipusok

Phishing Támadás: Célja és Fajtái

FAJTÁI

A phishing támadás (adathalász) célja, hogy az áldozattól bizalmas információkat szerezzen meg, például jelszavakat, bankkártya adatokat, vagy más személyes információkat.

Email Phishing - Adathalász e-mailek

Az egyik legelterjedtebb módszer, ahol a támadók hamis e-maileket küldenek, amelyek hitelesnek tűnnek, de valójában csalók által készített linkeket vagy mellékleteket tartalmaznak.
Cél: Az áldozatok rákattintanak a linkre vagy megnyitják a mellékletet, így hozzáférést biztosítanak a csalóknak az adataikhoz.

Spear Phishing - Célzottan

Célzott támadás, ahol a csalók egy adott személyre vagy szervezetre összpontosítanak, gyakran személyre szabott üzenetekkel.
Cél: Magas szintű bizalmas információk megszerzése, mint például céges adatok, vagy vezetői hozzáférések.

Whaling - Nagyhalakra

A spear phishing egy speciális fajtája, ahol a támadás célpontjai magas rangú vezetők vagy más befolyásos személyek (pl. CEO-k).
Cél: Nagy értékű információk vagy pénzügyi tranzakciók kicsikarása.

Halászat végtelen számú hálóval...

Védekezés Phishing ellen

MI

- Védekezés: ne adjunk meg felelőtlenül, vagy töröljünk minden olyan adatot, amely tálcán kínálja a lehetőséget annak, aki rossz szándékkal közelít felénk!

- Jó példa erre a pontos születési dátum, a telefonszám, a személyes e-mail cím ne legyen közszemlére téve

- Módosítsuk az adatvédelmi beállításokat!

- Állítsuk privátra a profilunkat: az a legbiztosabb, ha a közösségi média adatlapunk lényegi része csak a visszaigazolt ismerősök, engedélyezett követők számára látható.

- Érdemes a posztjaink láthatóságát is szigorúan korlátozni és kerülni a helymegosztás használatát.

- Kétfaktoros azonosítás a belépésnél (pl. Sms, Telefon vagy Egyszer használatos extra biztonsági kód)

Tudatosság Tudatosság Tudatosság

Malware fajták - "Károkozásra teremtve"

FAJTÁI

1. Vírus

Egy önmagát másoló kártevő program, amely egy másik programhoz csatolódik, és annak futtatásakor aktiválódik. Károsíthatja a rendszereket, adatokat törölhet vagy megsemmisíthet.
Cél: Rendszerek megfertőzése és károkozás, reprodukció.

2. Féreg (Worm)

Olyan önállóan működő malware, amely hálózatokon terjed anélkül, hogy egy másik programhoz kellene csatolódnia.
Gyorsan terjedhet, és jelentős hálózati erőforrásokat foglalhat le.
Cél: Rendszerek megfertőzése és terjedés.

3. Trójai program (Trojan Horse)

Olyan malware, amely hasznos szoftvernek tűnik, de rejtett rosszindulatú funkciókat tartalmaz. A felhasználó tudta nélkül káros tevékenységeket végezhet a háttérben.
Cél: Hozzáférés megszerzése a rendszerekhez, adatlopás, vagy további malware telepítése.

4. Kémprogram (Spyware)

Olyan malware, amely titokban gyűjt információkat a felhasználóról, például böngészési szokásokat, jelszavakat vagy pénzügyi adatokat,
majd ezeket továbbítja a támadónak.
Cél: Adatgyűjtés és lopás.

5. Adware

Reklámok megjelenítésére használt malware, amely különböző hirdetéseket juttat el a felhasználókhoz, gyakran a beleegyezésük nélkül.
Ezek a programok gyakran lassítják a rendszert.
Cél: Reklámbevételek generálása a felhasználók manipulálásával.

Man-in-the-Middle támadás (MitM)

MitM

Kérlek Marika most ide utalj légyszi!

Hogyan működik a támadás?

MitM

- **Adathalászat**: A támadó közbeékelődik egy felhasználó és egy weboldal, szolgáltatás vagy hálózat között, hogy megszerezze a kommunikációt (pl. jelszavakat, pénzügyi adatokat).

- **Wi-Fi lehallgatás**: Nyilvános Wi-Fi hálózatokon a támadó hamis hozzáférési pontokat állíthat fel, amelyekre a felhasználók csatlakoznak, így a támadó monitorozhatja az adatforgalmat. (Korrupt wifi)

- **Session hijacking**: A támadó hozzáfér a felhasználó és a szolgáltatás közötti munkamenethez, és átveheti az irányítást. (Nem biztonságos weboldal és a gépünk közé lép be)

- **DNS hamisítás**: A támadó módosítja a DNS-kéréseket, hogy a felhasználókat hamis domainekre vagy weboldalakra irányítsa. (Eltéríti a kérésünk)

- **Belső szabotázs:** Egy rosszindulatú munkatársunk telepíti fel belsőleg.

Tudatosan figyeljünk a biztonságra!

Védekezés a támadás ellen

MitM

1. **Titkosított kapcsolat használata (HTTPS)**: Minden fontos webes kapcsolatot titkosított protokollon keresztül kell megvalósítani (HTTPS).

2. **Nyilvános Wi-Fi elkerülése vagy VPN használata**: Ha nyilvános Wi-Fi-t használsz, mindig használj VPN-t (Virtual Private Network), hogy titkosított alagúton keresztül böngéssz, így a támadók nem férhetnek hozzá az adatforgalmadhoz.

3. **Biztonságos hitelesítés és erős jelszavak használata**: Kétfaktoros hitelesítés (2FA) használata erősen ajánlott, mivel ezzel csökkenthető a kockázat

4. **Eredeti, megbízható szoftverek és böngésző kiterjesztések használata**: Mindig ellenőrizd, hogy a használt szoftverek és böngészők naprakészek legyenek, és csak megbízható forrásokból töltsd le azokat.

5. **Digitális tanúsítványok ellenőrzése**: Mielőtt érzékeny adatokat adsz meg egy weboldalon, ellenőrizd a böngésző címsorában, hogy a webhely tanúsítványa érvényes és megbízható-e (pl. zöld lakat ikon és HTTPS kapcsolat).

6. **DNSSEC használata**: A DNS-biztonsági kiterjesztések (DNSSEC) segítenek megvédeni a DNS kéréseket és válaszokat, megakadályozva a DNS hamisítási támadásokat.

7. **Email hitelesítés**: Használj hitelesítési szabványokat, mint például DKIM, SPF és DMARC, hogy megelőzd a hamisított e-maileket.

Etikus hacker támogatása másképp

ETIKUS

Fel van véve...?!

joos.attila@webmark.hu

Köszönöm szépen a figyelmet!

Köszönet továbbá:
Szabó Tímea (VMKIK)
Takács Tamás (VMKIK)
Fehér Tamás (Innoweb Kft.)
Pintér Zsolt (Nyugat-Pannon Vállalkozásfejlesztési Kft)

WWW.WEBMARK.HU