

Útikalauz online csalások ellen



Zalaegerszeg, 2025. szeptember 16.
Keresztury Dezső Városi Művelődési Központ



Digital Security
Progress. Protected.

SICONTACT 
biztonság a digitális világban



Csizmazia-Darab István [Rambo]

IT biztonsági szakértő

TARTALOM



- Csalások

- Deepfake

- Gyanús jelek

- Védekezés, megelőzés

Kezdjünk egy videóval!



1.animal-olymp.1.00.mp4



BANKI CSALÁSOK

- 2023. MNB 18 e átvert banki károsult, 23 Mrd forint kár
- 2025. I. negyedévben átlag 822 ezer Ft/csalás
- 2019: A bankkártya-csalási károkat (92%) a bankok viselték
- 2023. Első negyedév 83% ügyfél hiba, 1.6 milliárd HUF
- 2025. Az első kárt (first loss) a bank fizesse JAVASLAT
- 2025. július 1. A Központi Visszaélésszűrő Rendszer (KVR)

CÍMLAP / BELFÖLD / TÖBB MINT 51 MILLIÓ FORINTOT CSALTAK KI EGY 80 ÉVES FÉRFITŐL

Több mint 51 millió forintot csaltak ki egy 80 éves férfitől

HM • 2025. AUGUSZTUS 06., 18:08

A Tiszaújvárosi Rendőrkapitányság eljárást indított ismeretlen tettesek ellen, akik egy 80 éves férfitől megtévesztéssel és manipulációval összesen több mint 51 millió forintot csaltak ki – írta a [police.hu](https://www.police.hu).

Banki ellenőrzések gyengesége

- 1\$ a Vöröskeresztnek
- Tranzakciók párhuzamosan több országból
- Életszerűtlen minden pénz kivétele egyszerre
- Értesítés kellene, ha bővül vagy változik a 2FA telefonszám, vagy másik banki app példányt telepítenek
- **Hiányzik, ha valaki MINDEN tranzakciót szeretne jóváhagyni**



419-es "nigériai" csalások

- **Eredet:** 1588. "Spanyol fogoly" trükk
- **Sztori:** Állítólagos gazdag rokon/ismeretlen angol fogságban
- **Kérés:** Sürgős pénz a szabadulásért, titoktartás
- **Ígéret:** Bőkezű jutalom, akár házasság a "fogoly" lányával
- **Lényeg:** Érzelmekre és kapzsiságra épít
- **Példa:** Elon Musk nevében kérnek pénzt, állítólag duplázzák



Elon Musk

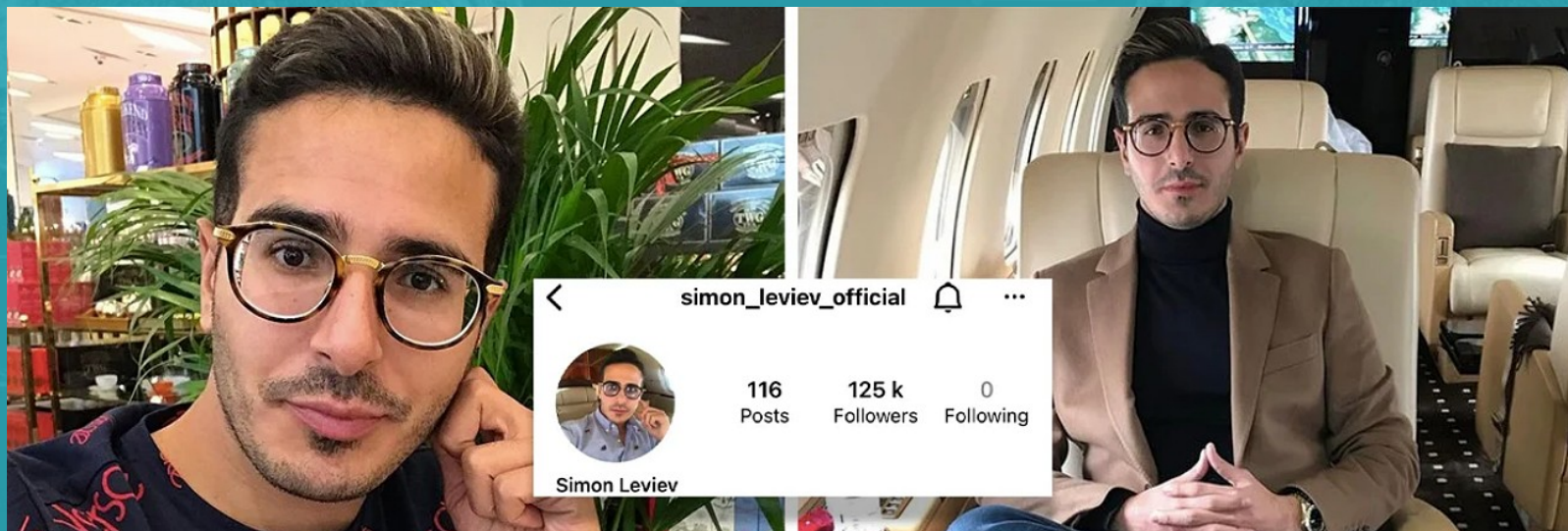
5000 BTC GIVEAWAY



If you send 0.1+ BTC, you will get 0.2+ BTC back
If you send 0.5+ BTC, you will get 1+ BTC back
If you send 1+ BTC, you will get 2+ BTC back
If you send 5+ BTC, you will get 10+ BTC back
If you send 10+ BTC, you will get 20+ BTC back

Romantikus csalások

- **Tipikus szereplők:** Fúrótornyos mérnök, katonatiszt, üzletember
- **Kapcsolatépítés:** Bizalmaskodó levelezés, romantikus üzenetek
- **Trükk:** Anyagi probléma (baleset, útiköltség), befektetési ajánlat
- **Kérés:** Pénz utalása, kriptovaluta vásárlása, számlanyitás
- **Cél:** Érzelmi manipuláció és gyors pénzszerzés
- **Példa:** Simon Leviev, Tinder swindler (Netflix, 2022.)



Csomagja érkezett SMS csalások

Módszer: SMS a futárszolgálat nevében, linkkel

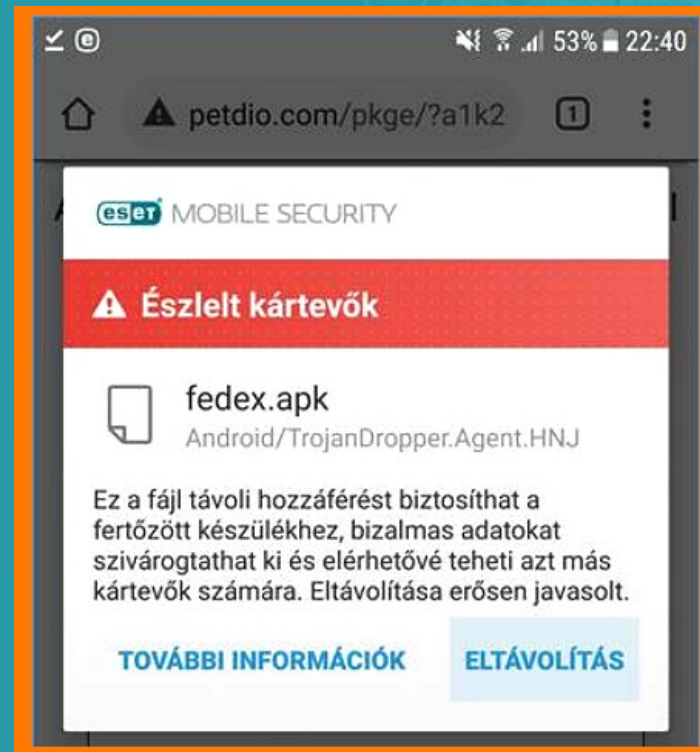
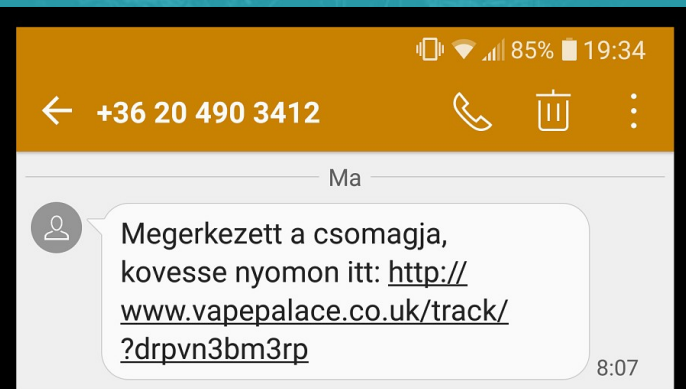
Csali: Sürgetés (24 óra, pótdíj)

Cél: Kártékony oldalra irányítani az áldozatot

Veszély: Banki adatokat lopnak,
vagy vírust telepítenek a telefonra

Kimenetel: Pénzlopás a számláról,
a készülék megfertőzése

Példa: 2021.03. tömeges SMS-ek
magyar számról, FedEx csalás



Csalások

Kimenetel: Adathalászat, távoli hozzáférés, pénz veszteség

10/35

2023. június Deepvoice virtuális emberrablás

- Jennifer DeStefano lánya nyári tábor
- Hívták a szülőket a lány hangján, hogy elhurcolják Mexikóba
- Elevenlabs hangklónozás

News | **Opinion** | **Sport** | **Culture** | **Lifestyle** | **More** ▾

Arizona

**Erum Salam**
Wed 14 Jun 2023 21.05 CEST

 **Share**

The Guardian



This article is more than **8 months old**

US mother gets call from 'kidnapped daughter' - but it's really an AI scam

Jennifer DeStefano tells US Senate about dangers of artificial technology after receiving phone call from scammers sounding exactly like her daughter

📷 Jennifer DeStefano at a Senate hearing in Washington DC on 13 June. Photograph:

Deepfake

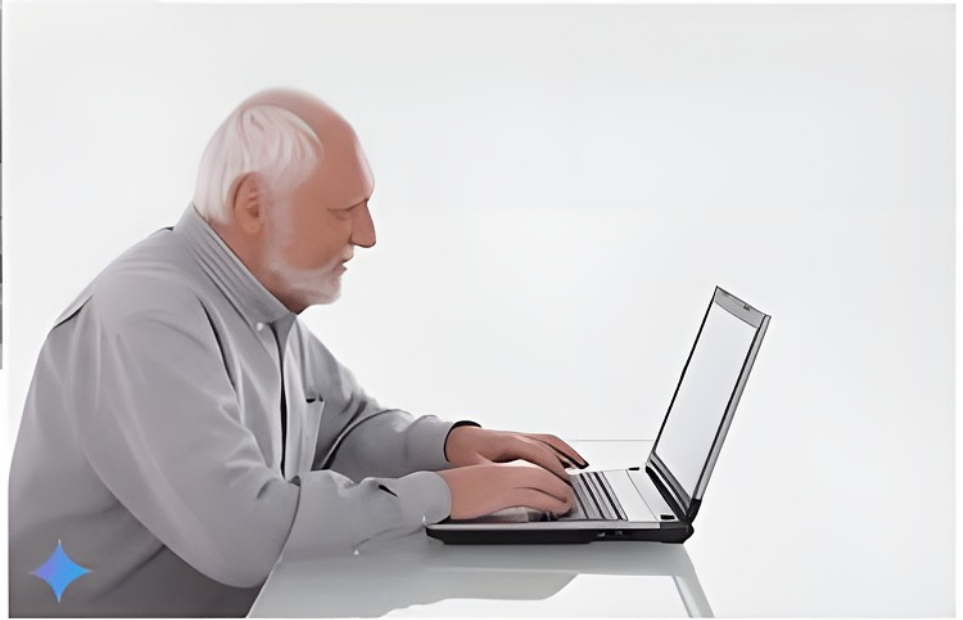


Bármi hamisítható: fénykép

Deepfake



Készíts oldalnézetet ebből a képből!



Google Gemini Flash 2.0

Bármí hamisítható: fénykép

Deepfake



Színezd ki a fotót!



Google Gemini Flash 2.0

Deepfake



aistudio.google.com



Bármí hamisítható: fénykép

Deepfake



aistudio.google.com



aistudio.google.com

Bármí hamisítható: fénykép

Deepfake



aistudio.google.com – Gemini 2.5 Flash Image (Nano Banana)

Deepfake



2.csdí-liveportrait.org.0.38.mp4





3.madeline.1.14.mp4



Egy autó kiállítás képei...

Deepfake



4.carshow.1.11.mp4



Támpontok: Generált videó felismerése

- Feltöltés dátuma: 2023. előtti?
- 10 másodpercnél rövidebb?
- AI vízjel/logo a sarokban?
- Nem látjuk ugyanazt a helyszínt más szögekből is
- A háttér tárgyak összevissza mozognak, vagy átfolynak egymáson
- Világítás, árnyékok, életszerűtlen furcsa mozgás



Támpontok: Generált videó felismerése

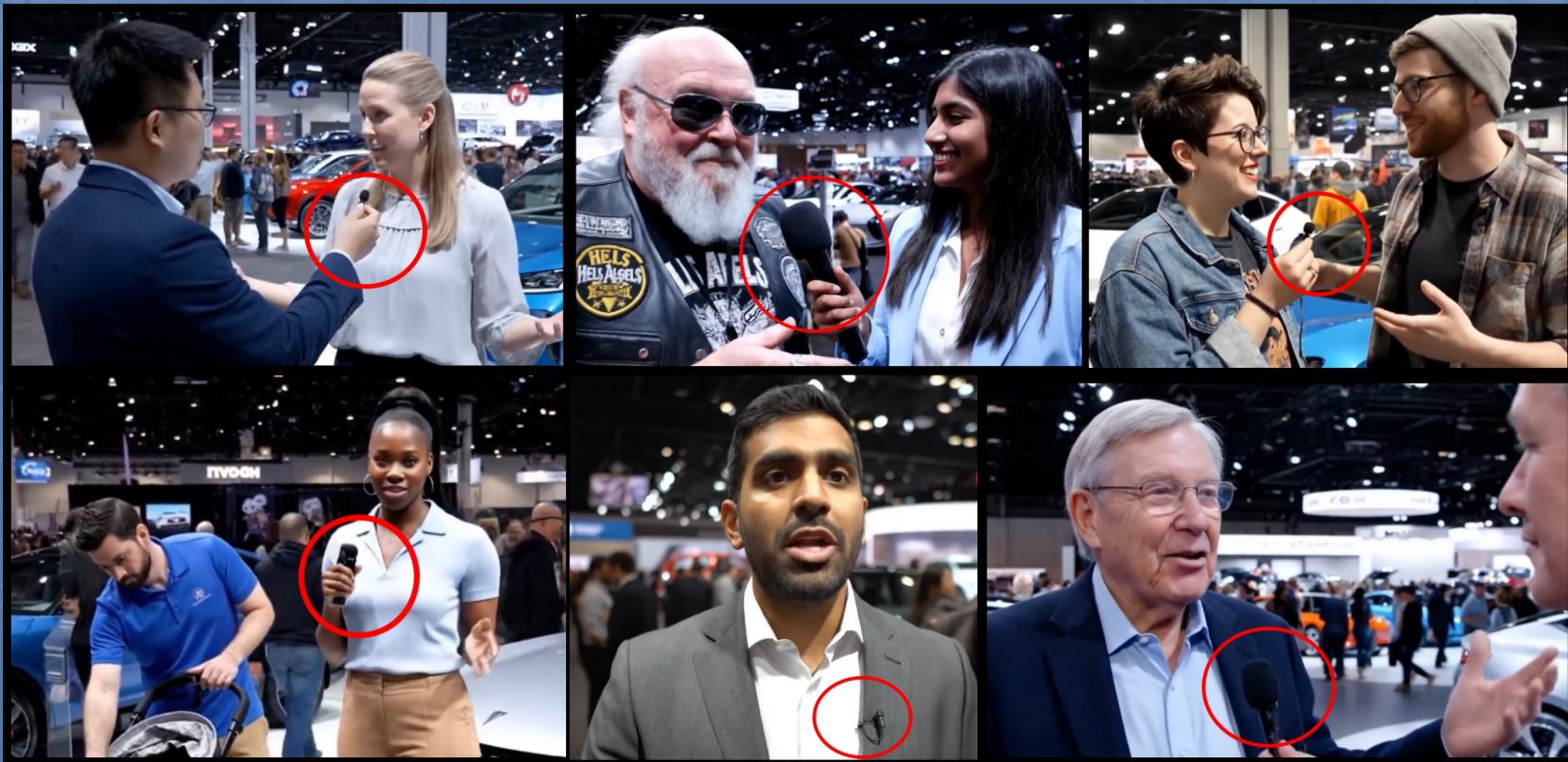
- Szemek, fogak hiánya-kidolgozatlansága, 6 ujjú kezek

Gyanús jelek



Támpontok: Generált videó felismerése

- Állandó szereplők apró változása: más ruha, más mikrofon



Támpontok: Generált videó felismerése

- Arcok vagy emberalakok durva elmosódása

Gyanús jelek



Támpontok: Generált videó felismerése

- Feliratokon nyelvi hiba vagy zagyva krikszkraksz karakterek



Támpontok: Generált videó felismerése

- Kimerevített kép durva kidolgozatlansága



Akkor teszteljük – igazi vagy sem?



5.kungfu.0.15.mp4

Akkor teszteljünk – igazi vagy sem?



6.esztergalyos.binnicula.0.29.mp4

Védekezés/megelőzés

- **Biztonságtudatosság:** kéretlen megkeresés, pénz- vagy adatkérés
- **Sose kattintsunk gyanús linkekre!**
- Bank, hatóság esetén **hívjuk vissza a hivatalos számon!**
- **Naprakész vírusirtó minden eszközre, hibajavító frissítések**
- **Erős egyedi jelszavak, 2FA, jelszó széf**
- **Sose küldjünk pénzt ismeretlennek!**
- **Élethosszig tanulás, tudás megosztás a családban**
- **Túl szép hogy igaz legyen, keressünk rá a neten, ChatGPT-n**

+49 173 4835604 >

Szöveges üzenet
ma 06:07

Posta: Onnek kifizetetlen
szallitasi koltsegei vannak. A
szallitas folytatashoz kerjuk,
ellenorizze weboldalunkat:
<https://posta-segotseg.com>

ChatGPT ▾

kaptam egy e-mailt a banktól, hogy gyanús utalást tapasztaltak

Ez nagyon komoly jelzés lehet, de sajnos az ilyen levelek nagy része **adathalász kísérlet** is lehet.

Első lépésként nagyon óvatosan kell kezelni:

1. Ellenőrizd a feladót

- Nézd meg pontosan az e-mail címét (nem csak a megjelenített nevet).
- Ha például egy „otpbank.hu” helyett „otp-bank-secure.com” vagy hasonló szerepel, akkor biztosan csalás.

2. Ne kattints a levélben lévő linkekre

- Az adathalász levelek tipikusan hamis banki bejelentkező oldalra visznek, ahol ellophatják az adataid.

Védekezés/megelőzés

ChatGPT ▾

megismerkedtem egy olajfúró tornyon dolgozó gazdag jóképű férfivel a neten

Ez az a tipikus helyzet, ahol nagyon óvatosnak kell lenni, mert az interneten rengeteg csaló használja a „gazdag, jóképű, külföldön dolgozó férfi” történetet – különösen az „olajfúró torony” vagy „katonai bevetés” háttérrel.

Miért gyanús ez a sztori?

- Az olajfúró torony mint munkahely klasszikus eleme az úgynevezett *romance scam* forgatókönyveknek.
- A csalók gyakran stockfotókat vagy más emberek képeit használják.
- Pár nap vagy hét után gyakran valamilyen „váratlan” pénzkérés következik (pl. haza akar jönni, de lefoglalták a papírjait, kell pénz a repülőre, vámra, engedélyre).

Védekezés/megelőzés

- **Revolut helyalapú biztonság** (location-based security) funkció: tranzakció csak ha a FIZIKAI BANKKÁRTYA (terminál) és a mobiltelefon egyazon fizikai helyen van. Kikapcsolható pl. pincében, kompon.
- Online fizetés csak virtuális kártyával, okos limitek, folyamatos bankkártya befagyasztás, push egyenlegértesítő
- **ESET Biztonságos bankolás:**
 - Böngésző-, billentyűzet- és vágólapvédelem, javascriptek ellenőrzése



Köszönöm a figyelmet :)

eset®



SIGONTACT
biztonság a digitális világban

www.antivirus.blog.hu, Hackfelmetszők podcast