

Internetes kockázatok és megoldások szülőknek



Szinyei Merse Pál Gimnázium 2026.02.17.

1988-ban kezdtem számítógép-programozóként dolgozni. Emellett vállalati vírusvédelmi felelősként is tevékenykedtem, majd 2000. óta már kizárólag vírusvédelemmel és számítógépes biztonsággal foglalkozom. 2007. óta vagyok a magyar ESET/Sicontact képviselőnél IT biztonsági szakértő. 2013. óta a gyermekek és szülők biztonságos internet oktatásában is aktívan tevékenykedem.



Csizmazia-Darab István [Rambo]
IT biztonsági szakértő



Helyzetkép 2026. február

AV-Atlas.org: 1.55 milliárd egyedi kártevő

TOTAL AMOUNT OF MALWARE AND PUA

Captured at: 2026/02/06 17:39 URL: <https://portal.av-atlas.org/malware>



1,800,000,000

AVTEST



Total Malware
1,557,663,304

Since 1984



1,500,000,000

1,200,000,000

900,000,000

600,000,000

300,000,000

0

2008

2009

2010

2011

2012

2013

2014

2015

2016

2017

2018

2019

2020

2021

2022

2023

2024

2025

2026

Helyzetkép 2026. február

Haveibeenpwned: 17.4 milliárd lopott/kiszivárgott jelszó

URL: <https://haveibeenpwned.com/>

Captured at: 2026/02/06 17:41

Have I Been Pwned

Check if your email address is in a data breach

Check

944

pwned websites

17,437,844,975

pwned accounts

Adathalászat

- Az AI segítségével bármilyen nyelven könnyen készíthető átverés
- Hihetőnek és hitelesnek tűnik
- A célzásnál és a testreszabásnál is használják az AI-t bűnözők
- Technikai tudás nélkül is profi csalás, 0-24-ben zajlik

BELFÖLD CSALÁS SMS KIBERVÉDELEM

A csomagküldős vírus itthon is tarolt

METAKING

2021.03.30. 20:19



Kövesse az Indexet
Facebookon is!



Követem!

Magyarországon sem kímélte az ügyfeleket a Spanyolországból indult csalóprogram. Ott 11 millió telefont fertőzött meg.

**ITTHON VOLT OLYAN KÁROSULT, AKINEK 4700 SMS-T KÜLDTEK EL A TELEFONJÁRÓL,
MIUTÁN LETÖLTÖTT EGY CSOMAGKÜLDŐS APPLIKÁCIÓT.**

Egy másik áldozatnak pedig több millió forintot emeltek le a bankszámlájáról, **számolt be** az RTL Klub híradója.

Banki csalások

- E-mail, sms, telefonhívás, fizetett keresési találat
- VOIP technológiával a hívószám is hamisítható
- Az AI segítségével bárkinek a hangja klónozható

The screenshot shows a search engine interface with the query "mbh bejelentkezés" in the search bar. The results are displayed on a dark background. A red rectangular box highlights the first result, which is a sponsored link. Below the box, another result for "MBH Netbank (korábban Takaréék)" is visible. The highlighted result includes a globe icon, the URL "login-ol1ne-mbhbanks.com", and a description in Hungarian encouraging users to log in quickly and safely. The second result includes the MBH Netbank logo and a description in Hungarian welcoming users and mentioning a phishing warning.

mbh bejelentkezés

Szponzorált

 login-ol1ne-mbhbanks.com
https://www.login-ol1ne-mbhbanks.com

M b h B a n k N e t b a n k : Login | Pénzügyei egy helyen

Jelentkezzen be M b h B a n k N e t b a n k fiókjába gyorsan, biztonságosan és kényelmesen.

 MBH Netbank (korábban Takaréék)
https://netbank.mbhbanks.hu

MBH Netbank (korábban Takaréék)

MBH Netbank (korábban Takaréék). Üdvözljük szolgáltatásunkban! **Bejelentkezés** jelszóval ... Az **MBH** Bank az utóbbi időben tapasztalt új csalási módszerekre ...

Online bankolás lakossági ...

MNB 2025. jelentés

- A második negyedévben 6 milliárd forint az okozott kár
- Egy ügyféltől átlagosan 2 millió forintot lopnak el
- A károk döntő részét - 90% - az ügyfelekre hárítják a bankok

24

24 EXTRA

Szőlő utca

Időjárás

5°C

HU

bűnügy

csalás

rendőrség

szekszárd

BELFÖLD

Döbbenetes csalással nullázták le 24 millió forintját egy szekszárdi nőnek

Vaskor Máté | 2025. 12. 17. 11:47

A napokban tett feljelentést a Szekszárdi Rendőrkapitányságon egy helyi nő, mivel megtudta a pénzintézeténél, hogy a számlaegyenlege nulla, a korábban ott elhelyezett 23 950 500 forintja nincs már meg, írja honlapján a rendőrség.

f

+

Befektetési csalások

- Túl szép hogy igaz legyen: gyors meggazdagodást ígérnek
- Hírességek arcával: engedély nélkül vagy generált AI tartalom
- Ismeretlen platformok, nyomásgyakorlás, sürgetés

← → ↻ https://rtlkl.com/products/9912

KÜLÖNLEGES BEJELENTÉS: Csányi Sándor legújabb befektetése miatt hitetlenkednek a szakemberek és félnek a nagy bankok

A magyar állampolgárok már több millió dollárt szedtek össze otthonról ezen "vagyonosodási kiskapuk" kihasználásával - de ez törvényes?

AS SEEN ON

HUNGARY today | DAILY NEWS HUNGARY | DUNA WORLD HD | 



OLVASÓK EREDMÉNYEI

PROFIT: 1205505 HUF



"Alig több mint 2 hete használom a **BitIQ** szoftvert. A kezdeti 250 dolláros letétemet 5802 dollárra növeltem. Ez sokkal több, mint amennyit a munkámmal keresek."

Kovács Bence
Győr

PROFIT: 1997596 HUF



2024. Seattle-Tacoma Nemzetközi Repülőtér

Vírústámadás miatt 1 hetes rendszerleállás: hivatalos weboldal, wifi, utastájékoztató, e-mail szolgáltatás megszűnt. Kézzel kellett 8 ezer poggyászt címkézni, beszállókártyákat írogatni.



Játékosok elleni támadások

- Neves platformokat támadnak: pl. Steam, Roblox, Minecraft
- Feltörik a fiókokat, anyagilag is megkárosítják őket
- Hamis frissítéseket, rosszindulatú kiegészítőket kínálnak

The Hacker News

1,500+ Minecraft Players Infected by Java Malware Masquerading as Game Mods on GitHub

👤 Ravie Lakshmanan 📅 Jun 18, 2025



A new multi-stage malware campaign is targeting Minecraft users with a Java-based malware that employs a distribution-as-service (DaaS) offering called [Stargazers Ghost Network](#).

"The campaigns resulted in a multi-stage attack chain targeting Minecraft users specifically," Check Point researchers Jaromír Hořejší and Antonis Terefos [said](#) in a report shared with The Hacker News.

"The malware was impersonating Oringo and Taunahi, which are 'Scripts and macros tools' (aka cheats). Both the first and second stages are developed in Java and can only be executed if the Minecraft runtime

Vírus és kémprogram elleni védelem

Proaktív védelem az online és offline fenyegetésekkel szemben.



INTERNET SECURITY



Kártevő eltávolítva

Egy kártevő (JS/Adware.Agent.CZ) volt észlelhető,
amikor a(z)  Google Chrome megkísérelt
hozzáférni egy webhelyhez
(d1f05vr3jsuy7.cloudfront.net).

A hozzáférés le van tiltva.

További információ erről az üzenetről



National Tax and
Customs Administration

Adóvisszatérítési értesítő

Tisztelt Adózó!

Ezúton értesítjük Önt, hogy az Ön által benyújtott 2025-es év személyi jövedelemadó bevallása alapján 140 000 HUF összegű visszatérítésre tarthat igényt. A Nemzeti Adó- és Vámhivatal feldolgozta az Ön beadványát és jóváhagyta a visszatérítést.

A visszatérítés részletei:

- Adóév: 2025
- Visszatérítendő összeg: 140 000 HUF
- Feldolgozás dátuma: 2026. január 26.

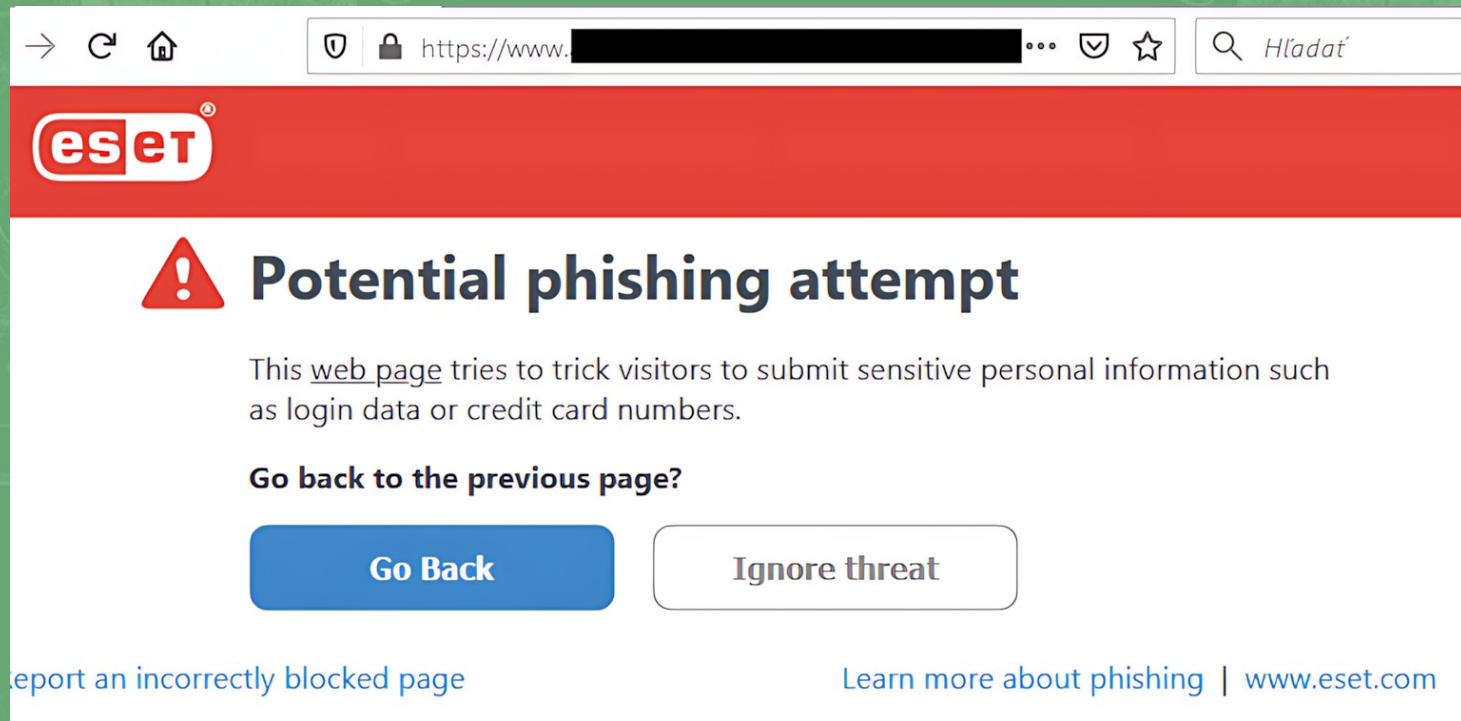
Teendők:

A visszatérítés igényléséhez kérjük, jelentkezzen be az ügyfélkapujába az alábbi gombra kattintva.

Belépés az ügyfélkapuba

Adathalászat elleni védelem

Blokkolja a csaló weboldalak kísérleteit, hogy azok ne tulajdoníthassák el az olyan, érzékeny adatainkat, mint például a felhasználónév, jelszavak vagy banki adatok



SMS-ben is érkezhethet az adathalász próbálkozás



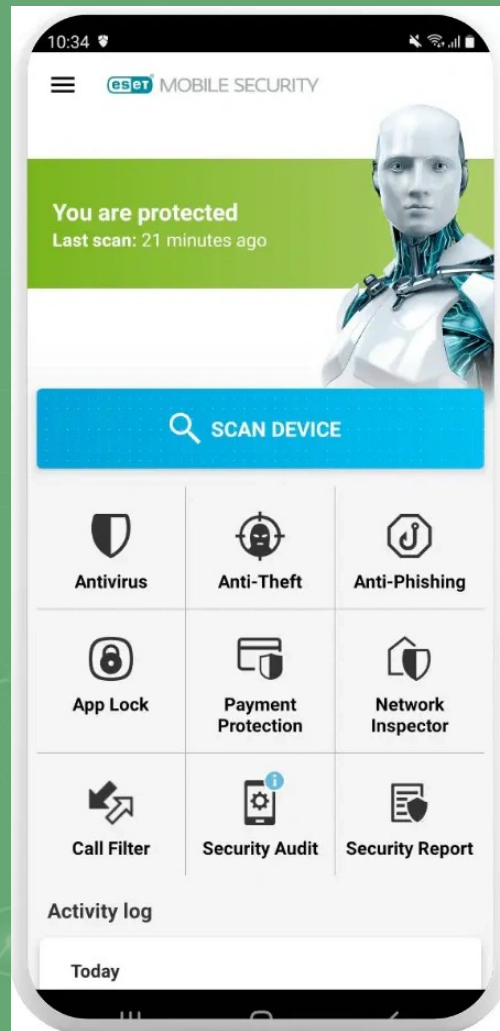
+49 173 4835604 >

Szöveges üzenet
ma 06:07

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

ESET Mobile Security

- Vírus- és adathalászat elleni védelem
- QR kódok ellenőrzése
- Fizetésvédelem
- Alkalmazás védelem
- Hálózatfelügyelet
- Adware detektor
- Hívásszűrés



Webkamerás kukkolás

2013. Egyesült-Királyság: 20 éves glasgow-i diáklányt, Rachel Hyndmant fertőzött laptopja kameráján kukkolták, képeket és videókat készítettek róla és feltöltötték az internetre

Charity warns parents to protect against webcam hacking

Murad Ahmed

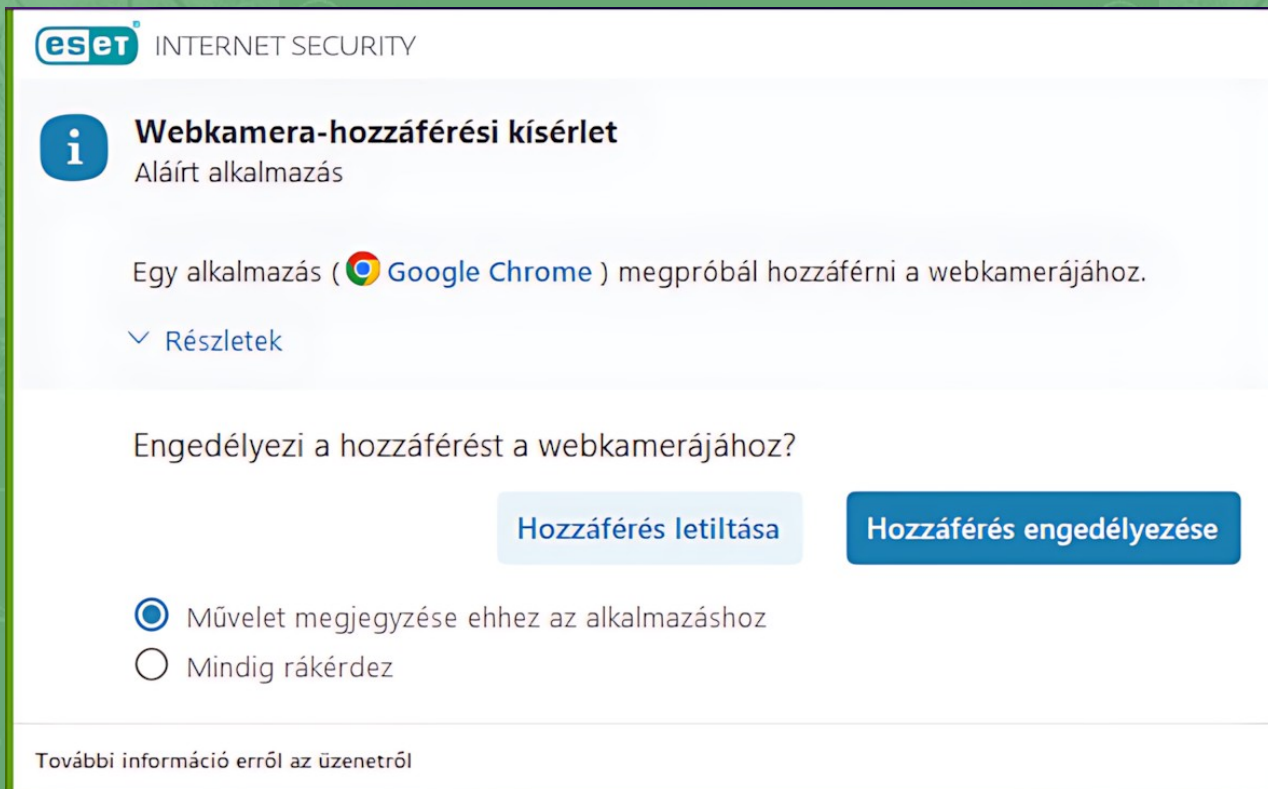
Friday June 21 2013,
1.01am BST, The Times



Though experts are unclear about how widespread the problem is, Rachel Hyndman, 20, a student from Glasgow, believes she is one of a growing number of victims of webcam hacking. She said that she spotted the camera on her laptop had switched itself on while she was using the machine to watch a film while in the bath.

Webkamera-védelem

Ha bármilyen alkalmazás illetéktelenül próbál hozzáférni a webkameránkhoz, arról riasztást kapunk, és blokkolhatjuk azt



Veszélyben a pénzünk

2016. Olyan kártevőt fedeztek fel, amelyik bankoláskor a memóriában észrevétlenül felülírja az átutalás célszámlájának számát, és így képes pénzt lopni az áldozatoktól

F5 Labs > Threats



FRAUD

Malware Targeting Bank Accounts Has a Swapping Pattern

By Doron Voolf & Elman Reyes

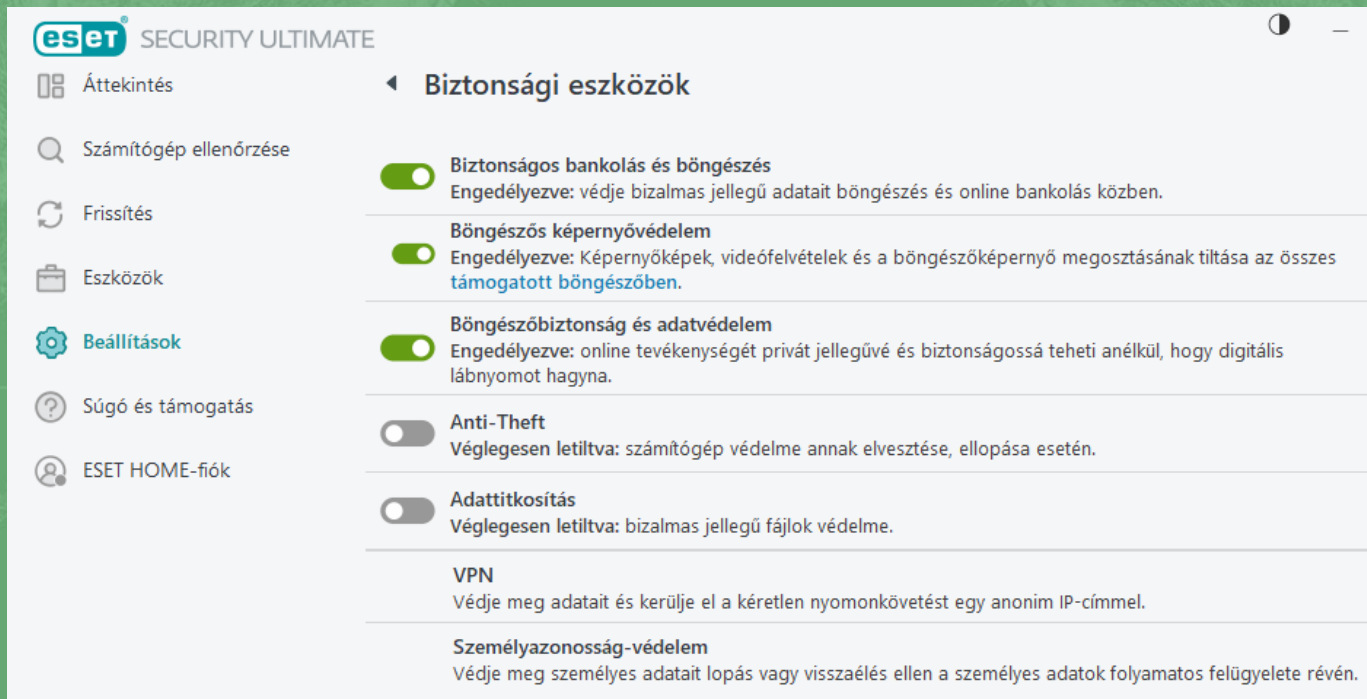
9/1/2016 • 4 min. read

F5 Labs analysts discovered a target pattern in the IBAN number formats as well as weekly changes to the script injection content. In May 2016, the F5 Security Operations Center (SOC) detected a generic form grabber and IBAN (International Bank...

In May 2016, we detected a generic form grabber and IBAN (International Bank Account Number) swap script injection targeting financial institutions across the world. IBAN swapping is a technique fraudsters use to first obtain access to an account, then exchange a legitimate

Biztonságos online bankolás

Biztonságos böngészőmód, amely automatikus védelmet nyújt az online bankolás és a webes kriptotárcákhoz való hozzáférés során. A billentyűzet és a böngésző közötti kommunikáció is titkosított, valamint védelmet nyújt a billentyűzetfigyelőkkel szemben is.



Zsarolóvírusok

2025. FBI jelentés: a csalók az USA-ban rekord évet zártak. Mintegy 16.6 milliárd dollár (5400 mrd HUF) értékben károsították meg vállalkozásokat és magánszemélyeket, ez a legnagyobb veszteség, amióta az iroda 25 évvel ezelőtt elindította az Internetes Bűncselekmények Bejelentési Központját (IC3).



WARNING: YOUR FILES HAVE BEEN LOCKED BY DEADBOLT

? What happened?

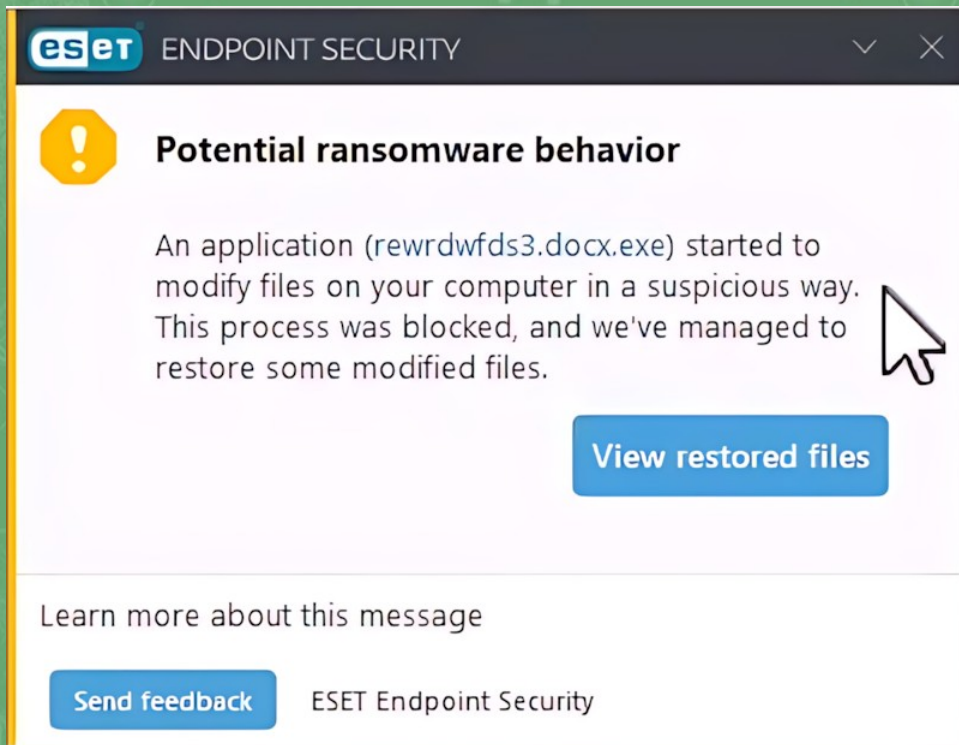
All **your files** have been encrypted. This includes (but is not limited to) Photos, Documents and Spreadsheets.

? What now?

You can make a payment of (exactly) 0.030000 bitcoin to the following address:
bc1q5q38z3qtleglms540yym5hsc9dz7g9yqp5ahzu

Ransomware elleni védelem és eltávolítás

Blokkolja azokat a kártevőket, amelyek titokban megpróbálják titkosítani az adatainkat. Többrétegű védelem a zsarolóprogramokkal szemben, fájlmentéssel és visszaállítással.



Ransomware elleni védelem és eltávolítás

Blokkolja azokat a kártevőket, amelyek titokban megpróbálják titkosítani az adatainkat. Többretegű védelem a zsarolóprogramokkal szemben, **fájlmentéssel és visszaállítással.**

eset ENDPOINT SECURITY

Restored files

Ransomware encrypted the following files, which have now been restored:

File	Last modified time
C:\A\Secreet\Annual-Report.docx	4. 10. 2024 10:29:18
C:\A\Secreet\CV.docx	4. 10. 2024 10:29:18
C:\A\Secreet\Financial-plan.docx	4. 10. 2024 10:29:18
C:\A\Secreet\Financial-report-2018.docx	4. 10. 2024 10:29:18
C:\A\Secreet\Financial-report-2019.docx	4. 10. 2024 10:29:18
C:\A\Secreet\Financial-report-2020.docx	4. 10. 2024 10:29:18

Close

Személyiség lopás

AZ EGÉSZSÉGÜGYI ADATLOPÁSOK



30%

Az egészségügyi adatlopások áldozatai közül 30% egyáltalán észre sem veszi, hogy áldozattá vált



3.7 millió Ft

Átlagosan ekkora számla érkezik, miután a csalók a nevünkben különféle speciális műtéteket, drága orvosi eszközöket vettek igénybe a lopott személyazonosságunk segítségével

10-ből 1



Csak minden tizedik megkérdezett áldozat érzi úgy, hogy az őt ért orvosi adatokkal kapcsolatos visszaélés végül megnyugtatóan zárult le

48%



A megkérdezettek 48%-a egészségügyi szolgáltatót váltana, ha elveszne, vagy ellopnák orvosi adatait



> 3 HÓNAP

Átlagosan 3 hónap telik el, amíg felfedeznek egy elloptott egészségügyi személyazonossággal kapcsolatos visszaélést



200 ÓRA

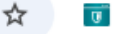
Átlagosan 200 órát tölt el az orvosi adatlopás áldozata utánjárással és ügyintézással, amíg sikerül tisztázni a bűncselekmény körülményeit



ENJOY SAFER
TECHNOLOGY™

- az áldozatok 30%-a észre sem veszi, hogy az adatait ellopták
- 3 hónap is eltelhet, mire a rendszerben észlelik a visszaélést
- átlagosan 3.7 millió forint kárt okoznak a csalók

Személyiség lopás elleni védelem

identityprotection.eset.com/app/dashboard

 IDENTITY PROTECTION

Let's Get Started

20% Complete

-  **Create your Profile**
For maximum protection, add as much information as possible.
-  **Add your Additional Information**
Add your Driver's License, Passport, Medical Insurance and Mother's Maiden Name to improve your Dark Web Monitoring.
-  **Add your Social Media Accounts**
Connect your Facebook, Instagram, Twitter or YouTube account to track and monitor your identity on social media platforms.
-  **Lost Wallet Assistance**
Quickly cancel and replace credit, debit, and ATM cards if your wallet is lost or stolen
-  **Discover Additional Resources**
Take advantage of these additional resources to set yourself up for success.

charges and order replacement credit cards by easily accessing your information online with Lost Wallet Assistance.

[View Wallet](#)

A védelem mellett a biztonság tudatosság is nélkülözhetetlen

- Óvatosság, egészséges gyanakvás és kételkedés, kritikus gondolkodás, felelősség, tanulási hajlandóság



Szia Anya!
Teljesen tönkrement a telefonom
ez az új számom, kérlek írd egy
üzenetet WhatsApp-on.
<https://wa.me/+36207735901>

Chainalysis 2026-os bűnügyi jelentése:

*"Az MI-vel támogatott csalások 4.5-szer jövedelmezőbbek,
mint a hagyományos módszerek"*

WhatsApp csalás

- Kártékony linket tartalmazhat
- Pénzt csalhatnak ki tőlünk
- Az ilyen SMS üzenetekre ne válaszoljunk!



RENDŐRSÉG
Szolgálok és Védünk

2025. 07. 02., sze - 08:41 Fejér Vármegyei Rendőr-főkapitányság

f Megosztás



Egy gárdonyi asszony több mint félmillió forintot utalt át egy csalónak, aki a lányának adta ki magát.

A napokban egy nyugdíjas nő tett bejelentést a rendőrségen arról, hogy – mint később kiderült – az SMS-ben érkezett „új szám” mögött nem a külföldön élő lánya, hanem egy csaló rejtőzött.

A jóhiszemű édesanya gyanakvás nélkül végül 550 000 forintot küldött egy megadott bankszámlára. A csaló ezután elérhetetlenné vált.

Fakenews 1.



Kertészné Bíró Erzsébet
körülbelül egy hónapja

🚌 A neve László, 60 éves. Közel negyven éve ugyanazon az útvonalon járja be Szeged utcáit. Ismer minden kanyart, minden megállót, minden arcot – bár sokak számára ő maga még mindig láthatatlan. Sosem késett. Sosem volt betegszabadságon. Nem panaszkodott, amikor télen nem akart becsukódni az ajtó, még akkor sem, amikor hátulról kiabáltak: „Hé, sofőr, életben vagy még?”

Fakenews 2.

- 2026 január: Meta bejegyzés egy Szegedi buszsofőről
- László állítólag munka közben elesett és kórházba került
- 34 ezer lájkot és 5000 megosztás, a kép generált

FACEBOOK, MESTERSÉGES INTELLIGENCIA, AI, ÁLHÍREK, FAKE NEWS



Kreatív 2026. január 08. 09:24

Rovat: Média

Egy kórházba került szegedi buszsofőrért aggódott több tízezer ember a Facebookon – kiderült, hogy a férfi nem is létezik

Egy magányos, kórházba került szegedi buszsofőr története futótűzként terjedt a közösségi médiában, több tízezen kívántak neki jobbulást. A probléma csak az, hogy sem a férfi, sem a történet nem valósak: a képek mesterséges intelligenciával készültek, az egész poszt pedig kitaláció volt.

Fakenews felismerés 1.

1960-as évek

ANALÓG KORSZAK



KERESD KI!

1980-as évek

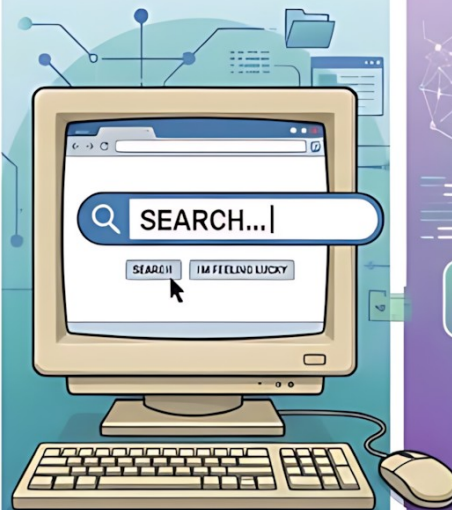
TELEFONOS KORSZAK



HÍVD FEL!

2000-es évek

INTERNETES KORSZAK



GUGLIZZ RÁ!

2025...

AI KORSZAK



KÉRDEZD MEG!

Fakenews felismerés 2.

- Kerüljük a kattintásvadász címeket!
- Érzelmi manipuláció felismerése: düh, ijedtség, fenyegetés
- Szerző, platform ellenőrzés, forráskritika, tényellenőrzés
- Fordított kép/videó keresés, URL ellenőrzés



Az AI segíthet a megelőzésben is 1.

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.

Az AI segíthet a megelőzésben is 2.

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).

+ 1 - Oversharenting

A szülők túlzott online megosztási szokása, amikor gyermekeik személyes adatait, képeit publikálják a közösségi médiában.

Mindez adatvédelmi és pszichológiai kockázat a gyerek számára.



shar·ent·ing

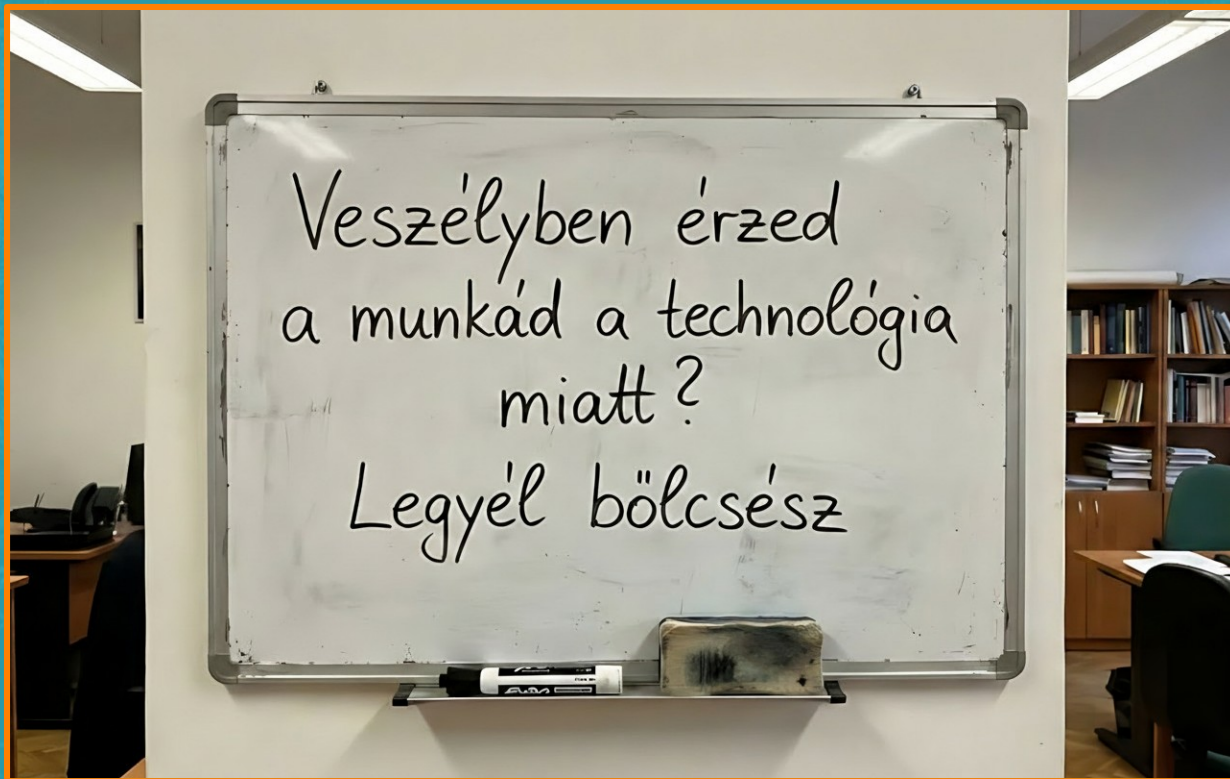
noun

When a parent or grandparent overshares information about their kids/grand kids on social media.

Üzenet a jövőből - Ellától



Köszönöm a figyelmet :)



- www.eset.hu/szuloknek
- Hackfelmetszők podcast

- antivirus.blog.hu
- info@sicontact.hu