



VIGYÁZZ, HA NEM TUDOD MI-T LÁTSZ!

Az AI veszélyei és káros hatásai napjainkban — deepfake, félrevezető tartalmak és AI-csalások

MI-t látsz Alapítvány · 2. előadás · 2026. augusztus 13. · Előadók: Németh Judit és Királyházi Csaba

IGAZ vagy HAMIS?

A most következő képeket és hangokat vajon az AI generálta?

Ha szerinted valamelyiket igen, akkor annál a diánál tedd fel a kezéd!



Golfozók, miközben mögöttük kitör a Kilauea - Mario Tama, Getty Images - 2018.05.16



Robbanás a Pentagonnál - AI generált kép - 2023.05.22



Légszennyezés - Robert Atanasovski/AFP/Getty Images - 2017.12.15



Jegesmedve invázió - Alexander Grir/AFP/Getty Images - 2018.10.13



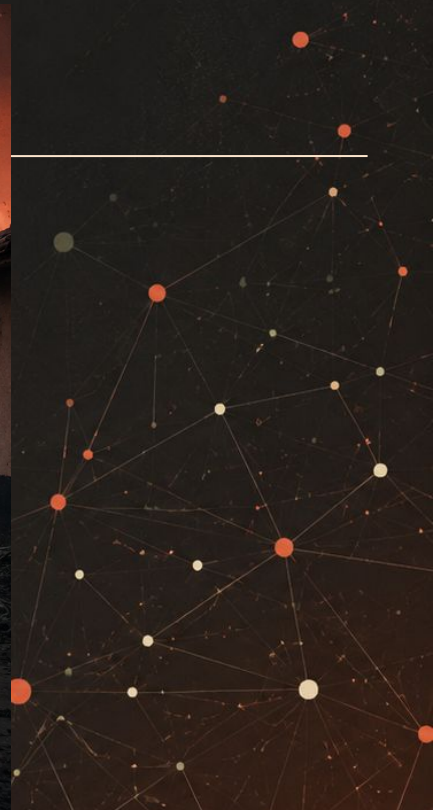
Tűzvész Los Angelesben - AI generált kép - 2025.01.09



Kislány egy kölyökkutyával a Helene hurrikán idején - AI generált kép - 2024.10.02



Egy házat elpusztító lávafolyam Hawaiiin - USGS - 1990.04.29



Menekülő lakosok - AI generált kép - 2026.08.10

**Csaba hangja
vagy AI?**



**Csaba hangja
vagy AI?**





Csaba előadás próba - AI generált videó és hang - 2026.08.11

Kik vagyunk?

Bemutakozás

- Az MI-t látsz Alapítvány egy független civil szervezet, ami az AI árnyoldalára próbálja felhívni a figyelmet: deepfake, félrevezető tartalmak, csalások, átverések, iskolai visszaélések, abúzus, és minden olyan káros jelenségre, amely az AI lehetőségeiből fakad.
- Ismeretterjesztéssel, oktatások szervezésével, könnyen érthető online tartalmak készítésével próbálunk minél nagyobb réteget megszólítani.
- Mi magunk is használjuk az AI-t a mindennapokban. Nem szeretnénk démonizálni ezt a forradalmi technológiát, csupán arra törekszünk, hogy etikusan és károkozás nélkül tegye hatékonyabbá a mindennapjainkat.



Miért vagyunk ma itt?

Célkitűzés

- Az első előadáson megmutattuk, hogyan működik az AI: hogyan jósol szavakat, miért téved magabiztosan, és hogyan generál képet. Ma azt nézzük meg, mi történik, amikor mindezt rosszra használják.
- Végigvesszük a legfontosabb csalási és félrevezetési formákat: a deepfake-videós befektetési csalásokat, a hangklónos telefonhívásokat, a tökéletes adathalász leveleket, a romantikus csalásokat és a gyerekeinket érintő visszaéléseket — mindegyiket valós, megtörtént esetekkel.
- És ami a legfontosabb: minden veszélyhez megpróbálunk védekezést is adni. Célunk a felkészítés, hiszen aki ismeri a trükköt, azt sokkal nehezebb átverni.

Egy kép, három különböző történet

Ugyanahhoz a tömegjelenethez három felirat tartozik. Melyik lehet igaz?

- Valemont főterén ünnepelték a szurkolók a Valegrad FC bajnoki címét
- Tízezrek tiltakoztak Valemont központjában az új belvárosi behajtási díj ellen
- Tűz ütött ki a valemonti koncerten, a résztvevők ezrei hagyták el a helyszínt.

A képből önmagában nem tudjuk eldönteni. Meg kell keresnünk az eredeti forrást, a helyszínt, az időpontot és más, egymástól független beszámolókat. A valós képhez is kapcsolható hamis történet.



Forrás, kontextus, szándék: a három erősebb kérdés

Félrevezetés

- Forrás: ki tette közzé először, és megtalálható-e az eredeti bejegyzés vagy felvétel?
- Kontextus: mikor és hol készült, és más megbízható források ugyanazt állítják-e?
- Szándék: mire akar rávenni a tartalom - pénzküldésre, adatátadásra, megosztásra vagy sürgős döntésre?

A három kérdés valódi és mesterséges tartalomnál egyaránt használható.

Az EU AI Act 50. cikke bizonyos AI-rendszerek és deepfake tartalmak esetén átláthatósági kötelezettségeket ír elő, de a csaló nem jelöl, a címke eltávolítható, a felvétel újratölthető, és a valódi tartalom is lehet félrevezető.

A jelölést kezeld hasznos jelként, ne hitelességi garanciaként.

Miért hisszük el a csalásokat?

Pszichológia

Minden működő átverés ugyanarra a néhány érzelmi gombra nyom rá — a technológia csak a kivitelezést tökéletesíti.

- Félelem: „baj van a gyerekeddel”, „letiltjuk a számládat”, „eljárás indult ellened”. A pánik kikapcsolja a mérlegelést.
- Kapzsiság és remény: „garantált hozam”, „csak ma”, „mindenki ezt csinálja”. A kimaradástól való félelem is ide tartozik.
- Szerelem és magány: a romantikus csalásoknál maga a kapcsolat a csali.
- Tekintélytisztelet: „a rendőrségtől hívom”, „a bank biztonsági osztálya vagyok”. A hivatalos hangnem önmagában engedelmességet vált ki.
- Segítőkézség: „csak egy gyors szívesség kellene” a jó szándékunkat fordítják ellenünk.

Az AI nem talált fel új csalást. A régi trükköket tette tökéletesebbé, olcsóbbá azoknak, akik a technológiát rosszra akarják használni.

Erős érzelem + időnyomás = vörös zászló

Ami tényleg fontos és valódi, az kibír öt percet.
A csaló nem bírja ki — mert az öt perc gondolkodási idő az ő legnagyobb ellensége.

Az AI az új eszköz az ártó szándék kezében

Eszköztár

Az AI ma már multimodális, vagyis szöveget, képet, hangot és videót is tud generálni vagy elemezni. A rossz szándékú AI használók pontosan ugyanezt a négy lehetőséget használják:

- Szöveg: hibátlan magyarsággal írt, személyre szabott adathalász üzenetek tömeggyártása. A törtmagyar „nigériai herceges” levelek kora lejárt.
- Kép: fotórealisztikus generálás, hamis profilképek, kamu termékfotók – és a hírhedt „meztelenítő” alkalmazások.
- Hang: néhány másodpercnyi mintából élethű hangklón, ami ma már valós idejű beszélgetésre is képes.
- Videó: deepfake – bárki arcával és szájmozgásával bármi elmondatható, egyre meggyőzőbb minőségben.

Mindez ma már nem igényel szakértelmet és pénzt: pár kattintással elérhető bárkinek. Ezért nem az a kérdés, hogy találkozunk-e ilyen átveréssel, hanem az, hogy mikor.

Mi teszi még hihetőbbé a csalást?

Eszköztár

Az AI használata nem csak a hétköznapi életünket, de a csalók dolgát is megkönnyítheti. Ezekkel az eszközökkel felvértezve sokkal gyorsabban, hatékonyabban és hihetőbben tudnak támadásokat elkövetni.

- Sebesség és mennyiség: rövid idő alatt sok emberhez juthat el a személyre szabott üzenet.
- Nyelvi minőség: az AI kijavítja a helyesírást, fordít és szakmai hangnemet is tud utánozni.
- Személyre szabás: az interneten fellelhető információk és a közösségi oldalak elemzésével és kutatásával, pontos neveket, kapcsolatokat és eseményeket építhet a történetbe.
- Multimodalitás: az e-mail mellé hangüzenet, kép, dokumentum vagy videóhívás társulhat.

Deepfake, hangklónozás, manipuláció

Fogalmak

- **Deepfake:**
Deepfake-nek nevezzük az AI-val létrehozott vagy lényegesen manipulált képet, hangot vagy videót, amely valós személyt vagy eseményt hitelesnek látszó módon jeleníthet meg.
- **Hangklónozás:**
A hangklónozás valaki hangjának ismertetőjegyeit, hangsúlyozását, tónusát, kiejtését utánozza. A másolatot rendszerint egy hangminta alapján készítik el. Minél hosszabb mintát szereznek, annál pontosabb hangklón készíthető.
- **Pszichológiai manipuláció:**
A pszichológiai manipuláció arra vesz rá, hogy önként adj át adatot, pénzt vagy hozzáférést.

A három részlet együtt különösen meggyőző és veszélyes eszköz egy rosszakaró kezében.

Mekkora a baj?

Kutatás

4,6 Mrd \$

ennyi pénz tűnt el kriptós csalásokban
egyetlen
év alatt a Bitget jelentése szerint
24%-kal több, mint egy évvel korábban
(2024-es felmérés)

40%

a nagy összegű csalásoknak már AI-deepfake
technológiát használt a jelentés szerint

971 181

adathalász esetet regisztráltak világszerte
2026 első negyedévében
ez negyedév alatt 14%-os növekedés (APWG)

**A csalás iparág lett: automatizált, méretezhető és személyre szabott.
A védekezésünknek is ehhez kell igazodnia.**

A támadás anatómiája

Elemzés

Ha folyamatként nézzük a támadást, több ponton is megállíthatjuk.

- **Információgyűjtés:**

A támadó közösségi profilokból, korábbi adatszivárgásokból, nyilvános eseményekből vagy beszélgetésekből nevet, kapcsolatot, szokást és aktuális élethelyzetet gyűjt. Attól, hogy valaki tudja a gyermeked nevét, a bankod nevét vagy egy közelgő utazásodat, még nem biztos, hogy az, akinek mondja magát.

- **Megszemélyesítés:**

A csaló (szerepe szerint) lehet családtag, banki ügyintéző, futár, rendőr, munkáltató, romantikus partner vagy közismert személy.

A szerephez illő nyelvet, arcot, hangot és dokumentumot használhat. A kijelzett telefonszám, a valódi logó vagy akár a valódi e-mail-fiók sem zárja ki a támadást. A fiókot feltörhették, a hívóazonosító megtévesztő lehet, az AI pedig már egy fotó alapján élő videóképet is tud generálni.

A támadás anatómiája

Elemzés

Ha folyamatként nézzük a támadást, több ponton is megállíthatjuk.

- **Érzelmi nyomás:**

A támadó a félelmedet, szégyenérzetedet használja, miközben sürget, titoktartást kér tőled vagy az együttérzésedre apellál, esetleg kihagyhatatlan ajánlattal kecsegtet. Sokszor hatóságok nevében keresnek meg, tekintélyt sugallva. A nyomás célja, hogy a megszokott ellenőrzési lépéseket felesleges késlekedésnek érezzük. Minél sürgősebbnek tűnik a kérés, annál fontosabb megállni.

- **Kívánt cselekvés:**

A támadás végül mindig valamilyen cselekvésre irányul: utalj pénzt, add meg a jóváhagyó kódot, nyiss meg egy linket, telepíts távoli hozzáférést, küldj intim tartalmat vagy oszd tovább a történetet. Ez a legjobb megállítási pont. Nem kell bizonyítanod, hogy a másik fél csaló. Elég, ha a kérést nem teljesíted addig, amíg egy másik irányból meg nem bizonyosodtál a történet valóságától.

Sztárok, akik ezt sosem mondták

Befektetési csalások

Nézzünk meg néhány konkrét csalási formát. Elsőként a befektetési csalást.

Magyarországon dokumentáltan készültek deepfake reklámvideók ismert emberek arcával és hangjával: többek között Szikora Róbert, Halász Judit, Majka és Ábel Anita „ajánlott” így csodakrémet, fogyókúrás tablettát vagy éppen befektetési platformot a tudtuk és beleegyezésük nélkül.

Nemzetközi szinten Elon Musk és más ismert milliárdosok arca a leggyakoribb csali, jellemzően kriptobefektetési „lehetőségekhez”.

Fontos kimondani: az érintett hírességek maguk is áldozatok – a nevükkel és az arcukkal élnek vissza. A rendőrség szerint az ilyen visszaélés személyes adattal visszaélés és csalás is lehet egyszerre, és a kár nagyságától függően akár 10 évig terjedő szabadságvesztéssel büntetendő.

A befektetési átverés forgatókönyve

Befektetési csalások

1. Hirdetés a közösségi médiában: ismerős arc, szenzációs ígéret — „a bankok titkolják!”.
2. Profin kinéző oldal: kamu cikkek, ellopott hírportál-arculatok, kitalált felhasználói vélemények.
3. Kis összegű „próbabefektetés”: néhány tízezer forint — pszichológiai belépő, mert ezzel már elköteleződöttünk.
4. Kamu hozamkimutatás: a felületen szépen nő a „nyereség”, gyakran egy kedves „személyes tanácsadó” is hívogat.
5. Egyre nagyobb befizetések — és amikor pénzt vennénk ki, előbb „adót” vagy „kezelési költséget” kérnek. Aztán mindenki eltűnik.

Egy új jelenség: a csalók visszatérnek a már kifosztott áldozatokhoz — magukat hatóságnak vagy banknak kiadva „segítenek visszaszerezni” a pénzt, természetesen újabb befizetésért cserébe. A pénzvisszaszerzést ígérő hívás maga is csalás.

Hogyan készül?

Befektetési csalások

Már ennyire egyszerű egy videó elkészítése, amiben valamilyen híresség vagy akár a saját családtagunk szájából halljuk, amit sosem mondott.



A hibavadászat hasznos lehet, de nem elég

Ellenőrzés

A furcsa kéz, szabálytalan fogsor, hibás tükröződés, szokatlan szemmozgás vagy hang-kép csúszás figyelmeztető jel lehet. Ezek azonban gyorsan változnak, és rossz minőségű valódi felvételen is megjelenhetnek.

Ha csak a képhibákra támaszkodunk, a jobb minőségű hamisítványt elhihetjük, a gyenge minőségű valódit pedig tévesen elutasíthatjuk.

- Kéz és fog: a generátorok hibázhatnak, de egyre ritkábban.
- Szem és száj: a pislogás vagy a hang-kép eltérése gyanús lehet, de a tömörítés és a rossz kapcsolat is okozhatja.
- Fény és árnyék: az ellentmondás segíthet, de szerkesztett valódi képen is előfordul.
- Vízjel vagy címke: hasznos, de eltávolítható, hiánya pedig nem bizonyít valódiságot.

„Anyá, segíts!” — az unokázós csalás 2.0

Hangklónos csalások

A klasszikus unokázós csalásban egy idegen adta ki magát családtagnak, síró, zaklatott hangon. A rendőrség évente több száz bejelentést kap, és egy-egy eset több millió forint kárt okozott.

Az AI ezt is új szintre emelte: már nem egy idegen hang állítja, hogy a gyermeked vagy az unokád – hanem tényleg az unokád hangján szól a telefon. Néhány másodpercnyi hangminta elég a klónhoz.

Már ennek a tükörképéről is hallani, vagyis a csalók a szülők hangját klónozzák, és a gyerekeket hívják megtévesztési céllal. Számhamisítás alkalmazásával a kijelzőn ráadásul a valódi szülő neve jelenik meg.

Hogy honnan van hangmintád?

TikTok-videó, Instagram-sztori, YouTube-szereplés, hangüzenet, a céges honlap bemutatkozó videója – vagyis szinte mindenkiről van.

Emlékszel a nyitójátékra?

Hangklónos csalások

Az előadás elején Csaba klónozott hangját mutattuk be, és még Csaba sem tudta volna eldönteni, hogy melyik az igazi.

Ha olyan hangklón készül rólam, amit én sem tudok megkülönböztetni a valótól, akkor honnan tudná az édesanyám?

Fontos etikai szabály, amit mi is betartunk: mi csak a saját hangunkat klónozzuk. Más hangjának klónozása – még viccből is – személyes adattal való visszaélés lehet.

Már nem bízhatunk a fülünkben és a szemünkben. A kritikus gondolkodásban és a felkészültségünkben bízhatunk egyedül, ehhez pedig szükség van a jelenség és a folyamat ismeretére!

Védekezés: a családi jelszó és a visszahívás

Hangklónos csalások

- Családi jelszó: egy előre megbeszélt szó vagy kérdés–válasz páros, amit csak a család ismer, és ami sehol nem szerepel az interneten. Ha a hívó nem tudja – bármilyen ismerős a hangja –, tedd le.
- Visszahívás az ismert számon: a bejövő hívás nem bizonyíték, mert a hívószám hamisítható. Tedd le, és te hívd a családtagot a telefonodban mentett számán.
- Ismerd fel a mintázatot: pánik + pénz + titoktartás („ne szólj apának!”) – ez a kombináció gyakorlatilag mindig csalás.
- Ellenőrző kérdés: olyan közös emlék, amit csak a valódi rokon tudhat. A családi jelszó biztosabb, mert az emlékek egy része kitalálható a közösségi médiából.

Ma esti házi feladat: beszélj meg otthon a családi jelszót. És hívd fel a szüleidet, nagyszüleidet is – nekik ez a tudás a legfontosabb védelem.

A tökéletes adathalász levél kora

Adathalászat

Az AI-val írt adathalász üzenet ma már hibátlan, személyre szabott és tömeggyártott. A támadások jelentős része már a nevünkön szólít meg és leggyakrabban banknak, csomagküldőnek, közműszolgáltatónak vagy hivatalos szervnek álcázza magát, mint amilyen a rendőrség vagy a NAV.

A közelmúltban az MBH Bank nevével visszaélő kampány két hónap alatt több mint 600 ügyfelet károsított meg!

A régi jó tanács – „figyelj a helyesírási hibákra” – mára elavult. Ami ma árulkodik:

- A sürgetés és a fenyegetés: „24 órán belül”, „azonnal letiltjuk”.
- Maga a kérés ténye: bank és hatóság SOHA nem kér jelszót, PIN-kódot vagy kártyaadatot üzenetben.
- A folyamat: váratlan üzenet + link + adatkérés = legyen mindig gyanús, akármilyen szép a kivitelezés.

Az AI mint testőr

Adathalászat

Az AI nemcsak a csalók eszköze, hanem a miénk is.

Próbáljuk ki együtt: mindenki nyissa meg a saját AI-ját (ChatGPT, Gemini, Copilot, Claude), és elemeztessen vele egy gyanús üzenetet ezzel a prompttal:

Prompt: Kaptam egy gyanús üzenetet. Értékelj, mennyire valószínű, hogy csalás! Sorold fel pontokba szedve, mi utal erre, és mondd meg, mit tegyek! Az üzenet:

Az AI jellemzően felismeri a sürgetést, a gyanús linket, az adatkérést és bárkinek, bármikor, rendelkezésre áll.

Két fontos kiegészítés az első előadás szelleméből: az AI válasza itt is **támpont, nem ítélet** — a döntés a tiéd. A gyanús üzenetben lévő linkre a bemásolás előtt se kattints rá!

Amikor a szív a célpont – az ál-Brad Pitt esete

Romantikus csalások

2025 januárjában járta be a világsajtót Anne, egy francia nő története, akitől 830 ezer eurót (mai árfolyamon nagyjából 330 millió forintot) csaltak ki másfél év alatt. Brad Pittnek kiadva magukat.

Az illúziót AI-generált fotókkal tartották fenn: volt köztük kórházi ágyon fekvő „Brad Pitt” is, akinek a „kezelésére” kellett a pénz, mert a „vagyonát zárolták a válása miatt”. Mindig volt logikus magyarázat – és mindig kellett még egy utalás.



A „ki lehet ilyen naiv?” kérdésre a helyes válasz: bárki, akit a megfelelő pillanatban, a megfelelő érzelmi gombnál találnak el. A magány mindenkit sebezhetővé tesz.

Az áldozathibáztatás a csalók legjobb barátja

Romantikus csalások

Amíg az áldozatok szégyellik magukat és hallgatnak, addig nincs feljelentés, nincs figyelmeztetés – és a csalók zavartalanul dolgoznak tovább. Aki ki tud állni és beszélni az esetéről, az másokat véd.

A romantikus csalás felismerhető mintázata:

- Hetekig-hónapokig csak beszélgetés: érzelmi függés épül, mielőtt bármi pénzről szó esne.
- Elszigetelés: „ez a mi titkunk” – a családdal és a barátokkal szembeni bizalmatlanság elültetése..
- Sosem tudunk találkozni, és a videóhívás is mindig megghiúsul – bár ma már a videóhívás is a csalókat segítheti..
- Előbb-utóbb mindig pénz kell: vészhelyzet, vám, ügyvédi költség, repülőjegy.

A legfájdalmasabb terep: a gyermekeink

Iskolai AI abúzus

1 200 000

gyermek számolt be egyetlen év alatt arról,
hogy a képeit AI-val szexuális tartalommal alakították
(UNICEF–Interpol–ECPAT kutatás, 11 ország)

minden 25.

gyereket érinti ez a jelenség egyes országokban,
az elkövető pedig nagyon gyakran egy osztálytárs

Magyar kutatás még nincs, de nincs okunk azt hinni, hogy nálunk más az arány. A „meztelenítő” appok ipara óriási: a hírhedt ClothOff alkalmazásnak 2024. év elején 27 millió felhasználója volt, napi 200 ezer generált képpel. Ahhoz, hogy egy fiatalt megzsaroljanak, nem kell valódi kép, a tudat és a látszat miatti szégyen épp elég.

Az intim deepfake akkor is valódi kárt okoz, ha hamis!

Mit tehet a szülő?

Iskolai AI abúzus

- Beszélgetés szégyenkeltés nélkül: a legfontosabb mondat, amit egy gyerek hallhat, hogy „hozzám bármivel jöhetsz, akkor is, ha hibáztál”. A gyerekek főként azért hallgatnak, mert szégyellik magukat és félnek a büntetéstől.
- Gondold át a megosztást: minden nyilvánosan feltöltött fotó nyersanyag lehet. Nézd át social média felületeidet, hogy kik láthatják a profilodat, az ott megosztott tartalmakat, akár gyermeked arcát.
- Ha megtörtént a baj: azonnal ments el mindent (képernyőképek, linkek, dátumok), majd jelentsd párhuzamosan a platformnak, az iskolának és a rendőrségnek. A generált kép készítése és terjesztése is bűncselekmény lehet.
- És a legfontosabb: a gyerek nem hibás – akkor sem, ha ő töltötte fel az eredeti fotót. A felelősség mindig az elkövetőé.

Ez az alapítványunk egyik fő fókuszterülete: jogi és lelki segítő hálózatot építünk, hogy a károsultakat a megfelelő szakemberhez irányíthassuk.

Mit tennél? – 1. helyzet

Kvíz

A lányod hív a saját számáról, sírva: balesetet okozott, azonnal utalnod kell 400 ezer forintot az ügyvédnek — és senkinek ne szólj róla.

A) Azonnal utalok, hiszen a hangja és a száma is az övé volt.

B) Leteszem, és visszahívom a telefonomban mentett számán — vagy rákérdezek a családi jelszóra.

C) Megkérdezem tőle, hol van, és további részleteket kérek a balesetről.

Szavazz a chatben: A, B vagy C?

Mit tennél? – 2. helyzet

Kvíz

Egy ismert üzletember videóban ajánl egy platformot, ami havi 30% hozamot garantál, és már 50 ezer forinttól lehet csatlakozni. A kommentek között sok a hálás vélemény.

- A) Kipróbálom a minimális összeggel — ennyit megér, és a videóban tényleg ő beszél.
- B) Megnézem az MNB-engedélyét, és ha az megvan, befektetek.
- C) Híres ember + garantált magas hozam = csalás. Jelentem a hirdetést, és továbblépek.

Szavazz a chatben: A, B vagy C?

Mit tennél? – 3. helyzet

Kvíz

SMS érkezik: „Csomagja vámkezelésre vár, kattintson és fizessen 990 Ft-ot.” És épp tényleg vársz egy külföldi csomagot.

- A) Kifizetem – kis összeg, és tényleg jön a csomagom.
- B) Nem kattintok: a futárcég hivatalos appjában vagy oldalán ellenőrzöm a saját követőszámommal.
- C) Válaszolok az SMS-re, és megkérdezem, melyik csomagról van szó.

Szavazz a chatben: A, B vagy C?

6 fontos dolog, ami ma elhangzott

Kvíz

1. Lassíts! A sürgetés a csaló legfontosabb fegyvere – ami tényleg fontos, az kibír öt percet.
2. Ellenőrizz másik csatornán! Hívd vissza az ismert számon, lépj be a hivatalos appba, kérdezd meg személyesen.
3. Beszéljétek meg még ma este a családi jelszót! És tanítsd meg a szüleidnek, nagyszüleidnek is.
4. Híres ember + garantált magas hozam = mindig csalás. Nincs kivétel.
5. Kérdezd meg az AI-t! A testőr-prompt bárkinek, bármikor, ingyen rendelkezésre áll.
6. Ha megtörtént a baj: nem szégyellnivaló, hanem bűncselekmény. Azonnal hívd a bankot, tegyél feljelentést, ments el minden bizonyítékot – és beszélj róla, mert ezzel másokat védesz.

A káros AI tartalmak ellen, a felelősségteljes AI használatért

Alapítvány

Az AI hasznos eszköz, és mi magunk is használjuk nap mint nap. Nem vagyunk AI-ellenesek, és nem is akarunk senkit lebeszélni róla.

A MI-t látsz alapítványt azért hoztuk létre, mert ugyanaz a technológia, ami hatékonyabbá teszi az életünket, visszaélésre is alkalmas: deepfake és megtévesztő tartalmak, hang és videó klónozással elkövetett csalások, iskolai AI-abúzus.

Az AI fejlődését nyomon követve folyamatosan kutatjuk, hogy mit lehet ma egy képpel, egy hanggal és egy videóval megcsinálni, ez hol árthat nekünk, és hogy mit tudsz ez ellen tenni.



Főbb tevékenységeink

Alapítvány

Ismeretterjesztés és edukáció: megmutatjuk, hogyan működik az AI és hogyan készül az AI-tartalom. Aki tudja, mi zajlik a motorháztető alatt, azt sokkal nehezebb megtéveszteni. Ez a mai alkalom is erről szólt.

Figyelemfelkeltő tartalmak: erősítjük jelenlétünket a közösségi média felületein, mert a kárt okozó anyagok is innen származnak. Célunk a figyelemfelhívás és a digitális ellenálló képesség erősítése

Személyes jelenlét: Igyekszünk felvenni a kapcsolatot az iskolákkal, beszélni tanárokkal, szülőkkel, gyerekekkel, ellátogatni az ország minden részére és szólni az idősekhez, és azokhoz, akik az AI technológiát még nem ismerik, mert ők különösen sérülékenyek lehetnek az ilyen megtévesztésekkel szemben

Támogatás: szeretnénk segíteni azoknak, akiket már ért olyan kár, amit közvetve az AI okozott. Jelenleg is építjük a jogi és lelki segítő hálózatunkat, hogy ha valakinek szüksége van segítségre, a megfelelő szakemberhez tudjuk irányítani.

Ha támogatnád a munkánkat

Alapítvány

Munkánk független, politikailag semleges és nonprofit.

A támogatások teszik lehetővé, hogy tevékenységünket szélesebb körben, hosszú távon és fenntartható módon végezhessük.

A támogatási lehetőségekről bővebben a www.mitlatsz.hu/tamogatas weboldalon tájékozódhatsz.

Keressük azokat a segítőket, együttműködő partnereket, akik hozzánk hasonlóan látják az AI sötétebb oldalát, és látnak kapcsolódást valamelyik tevékenységünkhöz.

Örömmel várjuk oktatók, tartalomgyártók, AI-szakértők, pszichológusok, jogi szakemberek, valamint minden olyan önkéntes jelentkezését, aki hisz abban, hogy közösen hatékonyan felléphetünk a káros AI-tartalmak terjedése ellen.

Mi jön ezután?

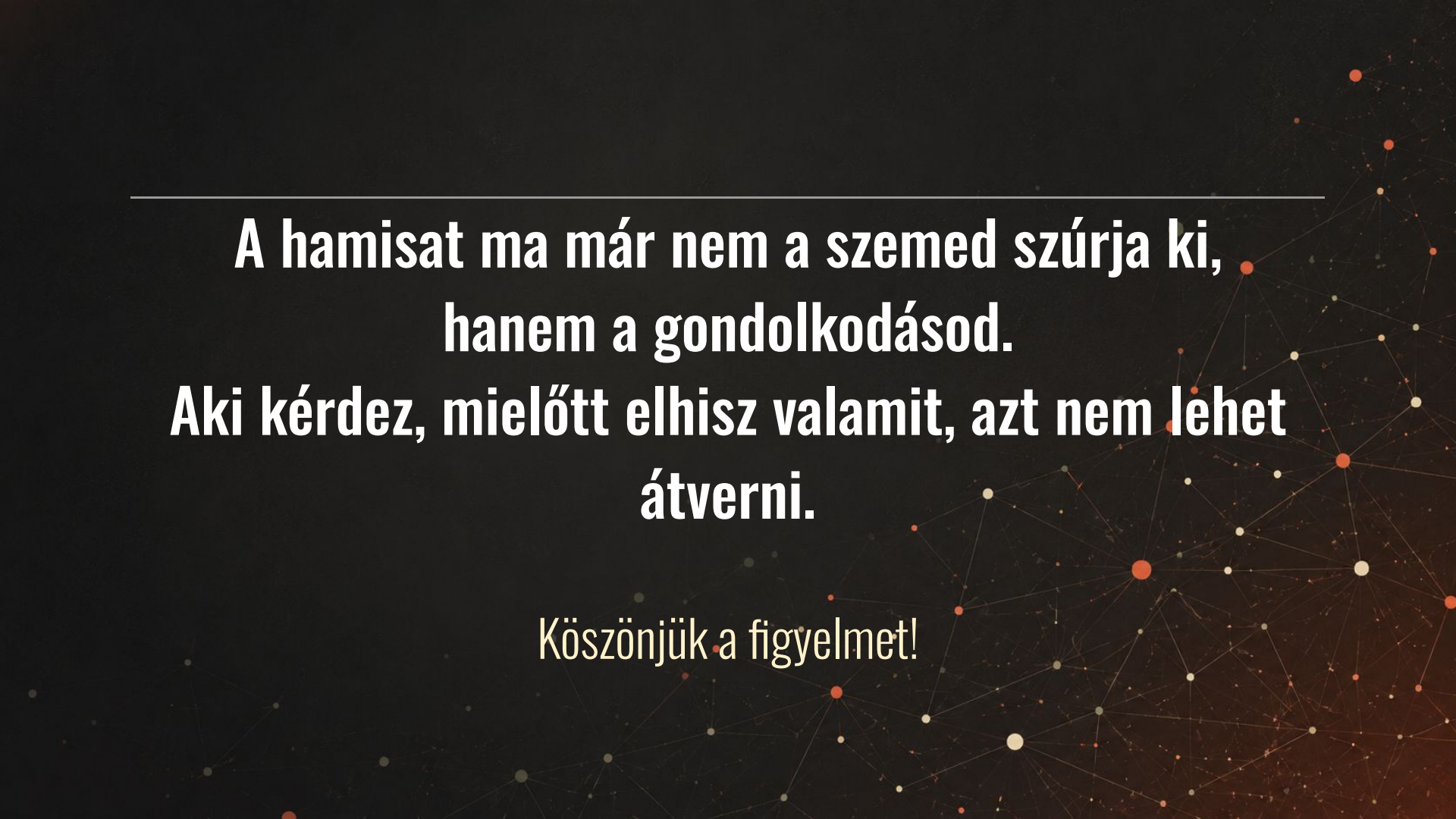
Folytatás

A sorozat záró előadása a munkahelyek világáról szól: ugyanezek az AI eszközök, csak most a cégek ellen fordítva.

- Hogyan hangzik egy vezetői hangklónos hívás, és mi az a CEO-csalás?
- Hogyan utalt el egy multinacionális cég pénzügyese 25 millió dollárt — közel 9 milliárd forintot — egy teljes egészében deepfake videókonferencia után?
- És mit tehet egy cég, egy csapat vagy akár egyetlen munkatárs, hogy ez ne náluk történjen meg?

MI-t látsz a munkahelyeden? — 2026. augusztus 17. (hétfő) 19:00–20:30, online.

Regisztrálni ingyenesen a <https://mitlatsz.hu/esemenyek> oldalon lehet.



**A hamisat ma már nem a szemed szűrja ki,
hanem a gondolkodásod.
Aki kérdez, mielőtt elhisz valamit, azt nem lehet
átverni.**

Köszönjük a figyelmet!