

Project: 101132954—DRONE—ERASMUS-EDU-2023-PI-FORWARD

Teacher and school leaders training to promote Digital literacy and combat the spread of disinformation among vulnerable groups of

A DRONE projekt célja képzési anyagok biztosítása az iskolák és szülők számára a digitális írástudás előmozdítására a dezinformáció elleni küzdelem érdekében a kiskamaszok körében.

Biztonságban egy bizonytalan világban

KEDVES SZÜLŐK!

A DRONE projekt keretében készítettünk kamaszoknak, valamint szülőknek szóló füzeteket a dezinformáció elleni küzdelem elősegítésére:

- Ez a füzet (**OLVASNI-Szülőknek**) a szülőknek készült, amelyben háttérinformációkat adunk a gyerekekkel történő beszélgetésekhez.
- Az **OLVASNI-Kiskamaszoknak** képregényt a szülőknek együtt kell átbeszélni a gyerekekkel!
- Az **OLVASNI-Tinedzsereknek** önálló feldolgozásra készült nagykaszok számára.

Az anyagok javítása érdekében várunk javító szándékú visszajelzéseket, amelyeket anonim módon lehet megadni:



Vagy

<https://tinyurl.com/DRONEvj>

Köszönjük a visszajelzést!

Készítette az ELTE DRONE csapata 2025 október (v.2025.10.24):

- Dr. Turcsányi-Szabó Márta, habilitált egyetemi docens (tszmarta@inf.elte.hu), az ELTE Informatikai Kar oktatási innovációért felelős dékáni biztosa
- Mikófalvy Franciska, pedagógus, az ELTE IK T@T Kuckó koordinátora

MJ: Az ötleteléshez és a képek generálásához felhasználtuk a ChatGPT 5.0-t.

Olvasnivaló szülőknek

A szülők kulcsszerepet játszanak abban, hogy megelőzzék az álhírek és félretájékoztatás terjedését a családjukon és a közösségen belül.

A szülőknek meg kell tanulniuk példát mutatni és tanítani a médiaértést, ösztönözni a nyílt és kritikus párbeszédet, felügyelni a digitális tevékenységeket, előmozdítani a felelős megosztást, használni az oktatási erőforrásokat, valamint együttműködni az iskolákkal és más szülőkkel. Ezzel képessé teszik gyermekeiket arra, hogy felismerjék, megkérdőjelezzék és ellenálljanak az álhíreknek – így növelve a digitális korban való ellenálló képességüket.

Ehhez a szülőknek meg kell tanulni és gyakorolni a következőket (lásd mellékletek):

Oktatási források használata és megosztása

- **Naprakészség:**
Tájékozottság az új dezinformációs formákról és azokról a platformokról, ahol a gyerekek időt töltenek. Beszéljük át melyek a megbízható híroldalak, mit jelentenek az egyes dezinformációval kapcsolatos kifejezések (lásd. **A. és B.**).
- **Játékok és eszközök használata:**
Használjunk interaktív forrásokat, például online teszteket, amelyek segítenek a gyerekeknek biztonságos környezetben felismerni az álhíreket (lásd **C.**).

Médiaértési készségek fejlesztése és példamutatás (lásd D., E., és F.)

- **Az ellenőrzés megértése és tanítása:**
Hogyan kell tény ellenőrzést végezni megbízható források segítségével, és bátorítani a gyerekeket, hogy ők is tegyék ezt. Gyakorolják együtt az információ pontosságának, manipulatív jellegének és hitelességének értékelését, például tényellenőrző weboldalak és böngészőbővítmények használatával.
- **Kritikus kérdések feltevése:**
Hogyan kérdezzenek rá az információ forrására, szemszögére és hitelességére. Hogyan gondolják át: *Ki készítette ezt? Miért? Megbízható? Mi hiányozhat vagy lehet manipulált benne?*
- **Jó példa mutatása:**
Hogyan érdemes megkérdőjelezni a forrásokat, értékelni az információt, és belátni, ha hibázott vagy hamis információt osztott meg. Kerülje el az ellenőrizetlen tartalmak megosztását!
- **Felelős megosztás tanítása:**
Állandó szokássá váljon az információ ellenőrzése megosztás előtt, és annak átbeszélése, milyen következményekkel járhat a hamis tartalom terjesztése.
- **Társas korrekció gyakorlása:**
Mit tegyünk, ha egy barát vagy családtag álhírt oszt meg? Hogyan lehet a beszélgetést kedvesen és építő módon megközelíteni?

A kiberbiztonság fontossága (lásd G.)

A kiberbiztonság a család információinak, magánéletének és eszközeinek védelmét jelenti az internet használata közben – különösen most, hogy a mesterséges intelligencia és az online technológiák mindennapossá váltak.

- **Személyes adatok védelme:** Meg kell tanítani a gyermekeket saját és mások adatainak (például fotók, nevek, iskola) védelmére, hogy megosztásuk milyen kockázatokhoz vezethetnek.
- **Csalások és manipuláció megelőzése:** Az online csalások és MI-alapú átverések gyerekeket is célzhatnak. Meg kell tanítani a gyermekeket, hogyan ismerjék fel a gyanús üzeneteket vagy kéréseket.
- **Illetéktelen hozzáférés megakadályozása:** Erős jelszavak, adatvédelmi beállítások és szülői felügyeleti eszközök segíthetnek megelőzni, hogy idegenek hozzáférjenek a fiókokhoz.
- **AI-adatgyűjtés hatásának csökkentése:** A mesterséges intelligencia gyakran adatokat gyűjt, sokszor anélkül, hogy egyértelműen beleegyezzünk. Tudatos döntésekre kell nevelni a gyereket.
- **Okos digitális szokások kialakítása:** Nyílt beszélgetésekkel és jó gyakorlatokkal élethosszig tartó biztonságos online viselkedést kell kialakítani.

Digitális tevékenységek felügyelete és irányítása

- **Kitettség figyelése és közvetítése:**
Különösen a kisebb gyerekek esetében be kell állítani az életkoruknak megfelelő korlátokat, és ha lehet, gyermekeknek szánt fiókokat kell használni.
- **Útmutatás, nem számonkérés:**
Ha kétséges tartalomba botlik vagy illetőt oszt meg, segíteni kell átgondolni a tartalmat, kijavítás vagy kritizálás helyett. Ez jó tanulási lehetőség!

Nyílt kommunikáció és kritikai gondolkodás elősegítésére

- **Rendszeres beszélgetés az online tartalomról:**
Tartsanak folyamatos beszélgetéseket arról, mit látnak a gyerekek az interneten - legyen szó influenszerekről, mémekről vagy virális történetekről. Használjanak valós példákat, akár a saját tapasztalataiból az álhírekkel kapcsolatban, hogy a téma érthetőbb legyen.
- **Nyitottság bátorítása:**
Legyenek nyitottak új ötletekre, hallgassák meg a különböző véleményeket, és vállalják be, ha tévednek.
- **A csoportnyomás megbeszélése:**
Értelmezzék miért fordulhat elő, hogy a beilleszkedés vágya miatt előfordulhat, hogy az emberek olyan információt is megosztanak, amiben maguk sem hisznek.

Együttműködés az iskolákkal és a közösséggel

- **Médiaértés oktatásának támogatása:**
Támogassuk, hogy az iskolák tanítsanak médiaértést és a kritikai gondolkodást a tanterv részeként.
- **Kapcsolattartás más szülőkkel:**
Osszák meg tapasztalatait és stratégiáját más szülőkkel, hogy támogató közösséget alakítsanak ki a felelős digitális állampolgárság érdekében.

JAVASLAT: A mellékletek oldalait egyenként ki lehet nyomtatni és poszterként a falra helyezni, hogy szem előtt legyen!

A. melléklet: Ajánlott olvasnivaló

„Az igazság nem hangosabb a hazugságnál — csak tudni kell meghallani.”

Hogyan ismerjük fel az álhíreket:

- <https://detekto.hu/szuloknek/>
- <https://kek-vonal.hu/tudastar/hogyan-ismerd-fel-az-alhireket>
- <https://www.urbanlegends.hu/2019/12/reuters-hogyan-ismerjuk-fel-a-deepfake-videok-at/>

Hasznos tanácsok szülőknek a család digitális biztonságáért:

- https://www.eset.com/hu/digitalis-biztonsag/szuloknek/?srsId=AfmBOooK-k_s7UIDr_eWi9qvmFhaxT5RhZGQBuhlB-R9EpSVMHJnE5YIK
- <https://digipedia.hu/>
 - o <https://digipedia.hu/cikk/hogyan-kezeljuk-a-dezinformaciort>
 - o <https://digipedia.hu/cikk/deepfake-most-mar-a-szemunknek-sem-hihetunk>
 - o <https://digipedia.hu/cikk/felretajekoztatás-informaciohamisítás-es-ezek-hatása-a-gyermekekre>
- https://gyerekaneten.hu/tema/A_jovo_nemcsak_az_Mle *Emberi készségek, amelyeket nem helyettesíthet a mesterséges intelligencia*

További hasznos linkek:

- <https://digitalisgyermekvedelem.hu/linkgyujtemenyek/> *Hasznos linkek*
- <https://unicef.hu/ezt-tesszuk-itthon/segitunk/helpapp> *Mobil app vészjelzésre*
- <https://kek-vonal.hu/tudastar/van-segitseg-e-learning-jatek-fiataloknak> *Van segítség! – játékos tanulás fiataloknak*
- <https://families.google/> *(a Google fordító beállítható a böngészőben a magyar nyelvű olvasásért) Megjegyzés: Google Family Link nem letölthető, ha egyszer felraktuk! A preventív szabályok betartása is jól működhet: mit tölthet le mobiljára a gyerek, vagy ha letöltött applikációt, akkor a szülő kapjon értesítést.*
- <https://www.urbanlegends.hu/tag/hoaxkviz> *(teszteld magad),*
- <https://www.urbanlegends.hu/2019/10/hogyan-ellenorizzunk-egy-informaciort-a-neten/>

Ajánlott posztok a gyerekekkel való beszélgetésekhez:

- https://storage.eun.org/resources/upload/310/20151103_150527260_310_HU_Think%20about%20your%20online%20contacts.pdf *Az összes online barátodat ismered személyesen?*
- https://storage.eun.org/resources/upload/255/20151103_144945066_255_HU_Think%20about%20the%20content%20you%20post.pdf *Gondolj arra a képre, amit posztolni akarsz!*
- https://storage.eun.org/resources/upload/046/20151103_140832134_46_HU-%20Think%20about%20how%20to%20protect%20yourself.pdf *Valaki bántó dolgot írt Rólad vagy Neked online*
- [https://storage.eun.org/resources/upload/172/20140220_103349714_172_Hungary_R\[1\].pdf](https://storage.eun.org/resources/upload/172/20140220_103349714_172_Hungary_R[1].pdf) *Tátika játék az internetes veszélyekről*

B. melléklet: Beszédes kulcsfogalmak

Digitális műveltség: Az a képesség, hogy hatékonyan, biztonságosan és kritikusan tudjunk digitális eszközöket és technológiákat használni.
Ide tartoznak olyan készségek, mint az online információk értékelése, weboldalak böngészése, alkalmazások használata, valamint a digitális jogok és felelősségek megértése.

A kiberbűnözés: Olyan bűncselekmény, amelyet számítógépek, okoseszközök vagy az internet segítségével követnek el.
Ezek lehetnek online támadások, csalások, adatlopások vagy zaklatások – tehát minden olyan tevékenység, amely a digitális térben történik és törvényt sért.

Kiberbiztonság: A digitális rendszerek, hálózatok és adatok védelme illetéktelen hozzáférés, támadás vagy károsodás ellen.
Magában foglalja a biztonságos jelszavak használatát, az online fenyegetések felismerését és a biztonságos online viselkedés követését.

Kritikai gondolkodás: Az a képesség, hogy világosan és logikusan gondolkodjunk, kérdőjelezzünk meg feltételezéseket, értékeljük a bizonyítékokat, és megalapozott következtetéseket vonjunk le.
Elengedhetetlen a tájékozott döntések meghozatalához és az álinformációk elleni védekezéshez.

Dezinformáció: Szándékosan hamis információ, amelyet arra hoznak létre és terjesztenek, hogy megtéveessenek vagy félrevezessenek embereket.
Példa: Hamis hírek, amelyek célja a közvélemény manipulálása.

Félreinformál: Hamis vagy pontatlan információ, amelyet nem szándékosan osztanak meg félrevezetés céljából.
Példa: Egy rosszul feliratozott kép megosztása úgy, hogy azt igaznak hiszik.

Káros információ: Valódi információ, amelyet azért használnak, hogy kárt okozzanak egy személynek, szervezetnek vagy országnak.
Példa: Bizalmas adatok kiszivárogtatása valaki megszegésére.

Álhír: Kitalált hírek, amelyeket legitim újságírásként mutatnak be, gyakran a közösségi médiában terjednek.
Példa: Vírusos címlapok, amelyek hamis tudományos felfedezéseket állítanak.

„Deepfake”: Szintetikus média (általában videó vagy hang), amelyet MI generál, hogy valós embereket imitáljon, gyakran meggyőző módon.
Példa: Egy videó, amelyen egy politikus olyan dolgokat mond, amiket sosem mondott.

Algoritmikus felerősítés: Az a mód, ahogy a közösségi média platformok algoritmusai növelik bizonyos tartalmak láthatóságát — néha akaratlanul is elősegítve a dezinformáció terjedését.
Példa: Szenzációhajhász vagy félrevezető posztok vírusossá válása az elköteleződésre fókuszáló algoritmusok miatt.

Visszhangkamra: Olyan online környezet, ahol az emberek csak olyan véleményekkel találkoznak, amelyek megerősítik a sajátjaikat, korlátozva a kritikai gondolkodást.
Példa: Egy közösségi média hírfolyam, amely csak egy politikai nézőpontot mutat be.

Megerősítési torzítás: Az a hajlam, hogy olyan információkat higgyünk el vagy osszunk meg, amelyek megerősítik meglévő nézeteinket, függetlenül azok valóságtartalmától.
Példa: Hiteles források figyelmen kívül hagyása, amelyek ellentmondanak a kedvelt véleményeknek.

Médiaműveltség: Az a képesség, hogy kritikusan elemezzük és értékeljük a médiatartalmakat, forrásokat és szándékokat.
Kulcsfontosságú, hogy a tanulók és felnőttek felismerjék és megkérdőjelezzék a dezinformációt.

Tényellenőrzés: Az információk megbízható források segítségével történő ellenőrzése megosztás vagy közzététel előtt.
Olyan szervezetek segítenek ebben, mint a Snopes vagy a PolitiFact.

Forrás megbízhatósága: A forrás megbízhatóságának megítélése a története, szakértelme és átláthatósága alapján.
Példa: Elsősorban peer-reviewed folyóiratokból származó információk használata anonim blogok helyett.

Digitális lábnyom: Az összes adat, amit egy személy az interneten maga után hagy, beleértve a megosztott tartalmakat, kommenteket és posztokat.
Tudatosan megosztani segít korlátozni a káros tartalmak terjedését.

Kiberbiztonsági tudatosság: A digitális fenyegetések — beleértve a dezinformációt is — megértése, mint a személyek és intézmények online védelmének része.
Magában foglalja a phishing felismerését, a manipulációt és a média hamisítást.

Gyűlöletbeszéd: Olyan beszéd, írás vagy tartalom, amely egy személyt vagy csoportot faji, vallási, etnikai, politikai, nemi, szexuális irányultság vagy más identitás alapján gyűlölettel vagy erőszakra uszítással támad.
Példa: "Az összes [etnikai csoport] csak bajt hoz ránk, ki kéne tiltani őket az országból!"

Részrehajlás: Olyan tudatos vagy tudattalan előítélet, amely például az egyik nemet előnyben részesíti a másikkal szemben — gyakran a nőket vagy nem-bináris személyeket érinti hátrányosan a médiában, munkahelyen, döntésekben stb.
Példa: Egy cikkben a férfi vezetőt „határozottnak”, a női vezetőt viszont „hatalmaskodónak” írják le ugyanazért a viselkedésért.

Trollkodás: Szándékosan provokatív, bántó vagy félrevezető kommentelés az online térben, azért, hogy érzelmi reakciót váltson ki vagy vitát gerjesszen.
Példa: Valaki egy természetvédelmi poszt alá azt írja: „Remélem, kivágják az összes fát, minek azok?”

Kattintásvadász tartalom: Olyan megtévesztő vagy túldramatizált cím, amely arra készteti az olvasót, hogy rá kattintson – akkor is, ha a tartalom nem azt nyújtja, amit a cím ígér.
Példa: „Sokkoló mit tett a kedvenc színészed – nem fogsz hinni a szemednek!”
(A cikkből pedig kiderül, hogy csak interjút adott.)

C. melléklet: Célszerű önértékelő

„Biztos hogy tudom: mit is tudok?”

Feladat: Kérjük, értékelje, mennyire érzi magát magabiztosnak az alábbi területeken az 1-től 5-ig terjedő skálán:

- 1 = Egyáltalán nem vagyok magabiztos
- 2 = Kicsit magabiztos vagyok
- 3 = Mérsékeltén magabiztos vagyok
- 4 = Magabiztos vagyok
- 5 = Nagyon magabiztos vagyok

Sorszám - Állítás X-eld be a megfelelőt! 1 | 2 | 3 | 4 | 5

1. Tudok segíteni a gyermekemnek erős és biztonságos jelszavak készítésében.
☐ ☐ ☐ ☐ ☐
2. Értem, hogyan kell bekapcsolni és elmagyarázni a kétlépcsős hitelesítést (2FA).
☐ ☐ ☐ ☐ ☐
3. Felismerem és el tudom magyarázni, hogyan néznek ki az adathalász csalások.
☐ ☐ ☐ ☐ ☐
4. Tudom, mi az a digitális lábnyom és miért fontos.
☐ ☐ ☐ ☐ ☐
5. Fel vagyok készülve arra, hogy beszéljek a gyerekekkel az álhírekről és félretájékoztatásról.
☐ ☐ ☐ ☐ ☐
6. Fel tudom ismerni a mesterséges intelligencia által generált tartalmakat (pl. deepfake-eket vagy hamis képeket).
☐ ☐ ☐ ☐ ☐
7. Otthon példát mutatok felelős megosztásra és tény ellenőrzésre.
☐ ☐ ☐ ☐ ☐
8. Tudom, hogyan vezesselem helyesen gyermekemet (ítélkezés nélkül), ha online hibát követ el.
☐ ☐ ☐ ☐ ☐
9. Használok eszközöket vagy weboldalakat annak ellenőrzésére, hogy az online információ igaz-e.
☐ ☐ ☐ ☐ ☐
10. Együttműködöm a gyermekem iskolájával vagy más szülővel a digitális biztonság vagy média-műveltség ügyében.
☐ ☐ ☐ ☐ ☐

Reflexió

Összegezze a pontszámokat.

Bármelyik 1-essel vagy 2-essel jelölt pont lehet jó kiindulópont a további tanuláshoz.

A 4-es vagy 5-ös pontszámok magabiztosságot jeleznek — szép munka!

Ha mégse, akkor olvassa el alaposan az összes mellékletet!

☒ **Szeretne tovább fejlődni? Tekintse át az állományban lévő anyagokat!**

D. melléklet: Dezinformációs játékok

„Jobb eljátszani, mint megélni és megjedni!”

1. Bad News Game (rossz hírek játéka)

 <https://www.getbadnews.com/>

Egy interaktív, angol nyelvű játék, ahol magunk válhatunk **álhírgyártóvá**, hogy megtanuljuk, milyen trükkökkel manipulálnak az interneten.

Cél: felismerni a manipulációs technikákat (clickbait, deepfake, érzelmi nyelvezet stb.).

- ✓ Fiataloknak és szülőknek egyaránt érdekes.
- ✓ Egyszerű angol, magyarul is jól magyarázható.

2. BBC iReporter

 <https://www.bbc.com/news/school-report-43391188>

A BBC játékos szimulációja, ahol **magunk lehetünk a hírszerkesztők**, és döntenünk kell, hogy mit osztasszunk meg a közösségi médiában.

Kihívás: felismerni az álhíreket és hamis tartalmakat.

- ✓ Interaktív, történet-alapú tanulás
- ✓ Médiatudatosságot fejleszt

3. Spot the Troll Quiz (Troll Felismerő kvíz)

 <https://www.spotthetroll.org/>

Egy online kvíz, ahol el kell döntenünk, hogy egy közösségi média profil **valódi emberhez vagy egy troll fiókhhoz tartozik-e**.

Cél: kritikai gondolkodás fejlesztése, megtanulni észrevenni a mesterségesen gerjesztett vitákat.

- ✓ Érdekes felnőtteknek is
- ✓ Jó beszélgetésindító családon belül

4. InVID & WeVerify Toolkit – kép- és videó ellenőrzés

 <https://www.invid-project.eu/tools-and-services/invid-verification-plugin/>

Bővítmény, amivel **képek és videók eredetét lehet ellenőrizni**, például deepfake-gyanús tartalmakat.

Használata: kicsit technikaibb, de szülői segítséggel a gyerekek is megérthetik.

- ✓ Komolyabb, de hasznos eszköz
- ✓ Oktatásban is használható

5. Real or Fake: Can You Spot Misinformation?

 <https://judgegpt.streamlit.app/>

Igaz vagy hamis: felismered a hamis információt?

- ✓ Kiváló szülőknek és nagyobb diákoknak

6. Tényleg! – Magyar tényellenőrző kvíz

 <https://tenyleg.hu/teszt/>

A **Tényleg.hu** magyar tényellenőrző oldal rövid, magyar nyelvű tesztjei és kvízei, amelyek bemutatják, milyen könnyű belefutni álhírekbe.

Cél: felismerni, hogy mi a hamis és mi az igaz egy hírben.

- ✓ Magyar nyelvű!
- ✓ Kiváló szülőknek és nagyobb diákoknak

E. melléklet: ELLENŐR

A gyerekekkel kell átbeszélni, hogy megjegyezzék!

Ellenőrizd a forrást

- Megbízható hírportálról van szó, vagy csak egy random fiókról?
- Az oldal vége “.com.co” vagy “.xyz”? (Ez intő jel lehet.)
- Más hitelesebb oldalak is ugyanerről számolnak be?

Tipp: Közösségi médián a feltöltő felhasználót is ellenőrizd!

Létező és megbízható forrásra hivatkozik?

A leírások gyakran tudományos adatokra hivatkoznak, amelyek vagy nem léteznek, vagy igazából mást igazolnak.

Tipp: Mindig ellenőrizd a forrást, amire hivatkozik és próbáld az is megérteni!

Lejárt a dátum?

A történet igaz, de évekkel ezelőtt történt — mégis úgy osztják meg, mintha most lenne.

Tipp: Mindig ellenőrizd az időbélyeget!

Ellenőrizd felismerő eszközökkel

Lásd a következő mellékletet!

Tipp: Gyűjts magadnak ellenőrző eszközöket, szükség lesz rájuk!

Nagyíts rá a képekre és videókra

Figyeld a furcsa kezeket, szemeket vagy háttereket (az MI könnyen elront részleteket).

- Árnyékok stimmelnek?
- A száj természetesen mozog a hanggal?
- Ékszerek reálisak és pl. fülbevaló mindkét oldalon ugyanaz?

Tipp: Nézd a videókat némítva. Ha így is „furának” tűnik, lehet, hogy hamis.

Őrizd meg a nyugalmad és olvasd tovább a címsoron túl

A címsor lehet kattintásvadász.

- Tényleg arról szól a cikk, amit a cím állít?
- Tele van CSUPA NAGYBETŰVEL, felkiáltójelekkel vagy túlzottan érzelmes?

Tipp: Ha túl örülten hangzik ahhoz, hogy igaz legyen – lehet, hogy tényleg nem az.

Reális, hihető tartalom?

- Logikus, amit állítanak?
- Van benne túlzás, szenzáció, sok felkiáltójel vagy csupa nagybetűs szöveg?
- Úgy hangzik, hogy „túl szép (vagy túl durva) ahhoz, hogy igaz legyen”?

Tipp: Az igazság nem siet – de a hamis hírek villámgyorsan terjednek.

Ne oszd meg, amíg nem ELLENŐR-izted!

F.melléklet: Felismerő eszközök

Megbízható online eszközök a hamis tartalmak ellenőrzésére

Megjegyzés: Érdemes a böngészőben aktiválni a Google Fordítót az oldalak magyar nyelven történő olvasásához!

1. Google Fact Check Explorer

<https://toolbox.google.com/factcheck/explorer/search/list:recent;hl=hu>

Olyan keresőmotor, ami megmutatja, hogy egy állítást már ellenőriztek-e. Kiváló idézetek vagy hírek ellenőrzésére.

✓ Hivatalos Google-eszköz, újságírók is használják.

2. InVID WeVerify Toolkit

<https://www.invid-project.eu/tools-and-services/invid-verification-plugin/>

Böngészőbővítmény, amely ellenőrzi a videók és képek eredetét. Fordított képkeresést végez, *deepfake* jeleket keres.

✓ Európai médiaszakemberek is megbíznak benne.

3. TinEye

<https://www.tineye.com/>

Fordított képkeresés: egy kép feltöltésével, megmutatja, az honnan származik. Segít felismerni a régi képeket, amiket hamis hírekhez használnak fel.

4. Snopes

<https://www.snopes.com/>

Lerántja a leplet a hamis pletykákról, álhírekről és átverésekről. Egyszerű, érthető magyarázatok - tökéletes tiniknek is.

✓ Több mint 20 éve megbízható forrás.

5. Media Bias/Fact Check

<https://mediabiasfactcheck.com/>

Megmutatja, mennyire elfogult vagy megbízható egy hírportál. Skálán osztályozza az oldalakat, és magyarázatot is ad.

G.melléklet: Gondolatébresztő a kiskamaszokkal való beszélgetésekhez

„Biztonságban egy bizonytalan világban”



A történetet adjuk oda a gyerekek elolvasására, majd indítsunk beszélgetést:

- Találkoztatok már hasonló helyzettel?
- Hogyan kezeltétek?
- Említetek olyan helyzeteket, ahol több háttérismeretre volt szükség az eset megfelelő kezeléséhez.

Szereplők:

Lia (14): Barátságos, nyitott, imád táncolni, rendszeresen posztol a TikTokon.

Rafi (15): Lia unokatestvére, csendes és technikailag jártas.

Juli néni: Menő könyvtáros, aki az iskola digitális klubját vezeti.

1. fejezet: A vírusos megemlítés

Lia izgatott volt. Épp most érte el a 10 000 követőt TikTokon a legutóbbi táncos videója. Több mint 18 000 megtekintés két nap alatt. Aztán jött egy **tag** (megemlítés).

„Omg, Ezt jól csináltad 🥰 nézd meg ezt is!” - és egy furcsa link.

Rákattintott. Semmi nem töltődött be. „Hm, talán elromlott.” Nem gondolt többet rá.

2. fejezet: Valami... nem stimmel

Aznap este később az egyik barátja írt neki:

„Hé... küldtél nekem egy furcsa videót??”

Aztán egy másik üzenet:

„Miért írogatsz mindenkinek nyereseményekről? Feltörték a fiókodat?”

Lia gyomra görcsbe rándult. A TikToka üzengetett a követőinek, pedig ő erről nem tudott. Lia pánikba esett, és felhívta az unokatestvérét, Rafit.

„Ne aggódj” - mondta Rafi. - „Ez történt más barátommal is. Adathalászatnak hívják.”

„Halászat?!” - pislogott Lia.

„Nem horgászbottal. Ez az, amikor csalók 'lehalásszák' az infóidat. Az a link valószínűleg rávette az appodat, hogy beengedje őket.”

Új jelszót állítottak be, bekapcsolták a kétfélcés (2FA) azonosítást, és Rafi segített bejelenteni a problémát.

„De miért pont én?” - kérdezte Lia.

„Mert rákattintottál” - mondta Rafi szelíden. - „Ez okos emberekkel is megtörténik.”

3. fejezet: A digitális klub

Másnap Lia még mindig zaklatottan ment az iskolai könyvtárba. Juli néni, a könyvtáros, észrevette. Lia mindent elmesélt.

„Nem is gondolkodtam. Csak egy **tag** volt. Olyan butának érzem magam.”

Juli néni kedvesen elmosolyodott.

„Nem vagy buta. Tanulsz. Ezért indítottuk a Digitális Élet Klubot. Csatlakozol?”

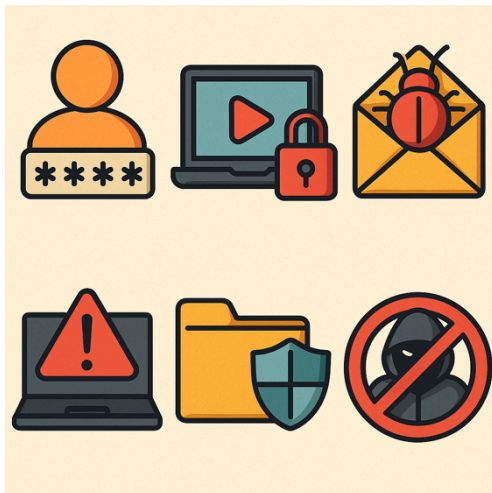
4. fejezet: Mit tanultam

Egy héttel később Lia a Digitális Klub előtt állt.

„Ijesztő, milyen gyorsan történt. De rájöttem... sosem gondolkodtam igazán azon, hogyan használom a közösségi médiát.” Felemelte a listáját ...

Miért fontos a kiberbiztonság (igen, neked is!)

„A kiberbiztonság nem a félelemről szól, hanem a szabadságról szól: önmagad lehess, megoszthass, kapcsolódhass és alkothass úgy, hogy ne piszkáljanak.”



Mi az a kiberbiztonság egyáltalán?

Gondolj a kiberbiztonságra úgy, mint a személyes higiéniára - csak a digitális életben.

Ahogy a fogmosás megóv a fogszuvasodástól, a kiberbiztonság megvéd a:

- Hackerektől, akik ellopják a fiókodat
- Furcsa idegenektől, akik látják az adataidat
- Fotók, házi feladatok vagy akár a személyazonosságod elvesztésétől

És nem - nem kell híres influenzszernek lenned, hogy célpont legyél. Ha online vagy, már benne vagy a "játékban".

Mi történhet, ha nem védekezel?

- A TikTok vagy Insta fiókodat feltörik, és spamet küld,
- Az e-mailedet használják más jelszavak visszaállításához,
- Kiszivárognak személyes fotók vagy üzenetek,
- Valaki másnak adja ki magát helyetted, és másokat ver át,
- A privát üzeneteid nyilvánossá válnak,
- Az iskolai emailjeidet feltörik
- Valaki rendel a nevedben
- Téged hibáztatnak olyan üzenetekért, amiket nem is küldtél.

👤 Igen, ez tényleg megtörténik. Nem csak " felnőtt probléma".

Hogyan védekezhetsz?

- Védd a fiókjaidat!
- Erős jelszó használata és ne használd mindenhol ugyanazt a jelszót!
- Ne dőlj be a pszichológiai manipulációnak!
- Legyél tisztában a MI dezinformációs felerősítő módszereivel!
- Használd minden esetben a Netikettet!
- Minimalizáld a digitális lábnyomodat!
- Állandósuljon benned az ELLENŐR-zés!
- Ne félj jelenteni, ha mások nem tartják be a védelmező szabályokat!
- Ismerd meg a negatív információ fajtáit!
- ismerd meg, miben menő és miben ciki az MI!
- Lásd be, miért lehet az MI túlhasználata veszélyes a tanulókra!
- Lásd be, miért fontos a tanulás (az MI mellett is)!

----- A továbbiakban ezekről bővebben lesz szó!

Hogyan legyél biztonságban a közösségi médiában?

„A közösségi média a TE tered. Te irányítasz!”



A közösségi média szuper lehet a szórakozáshoz, barátokkal való csevegéshez és mémek megosztásához – de könnyen kaotikussá válhat. Hackerek, zaklatók, furcsa privát üzenetek és hamis tartalmak mindenütt ott vannak. Így maradhatsz biztonságban és erős online:

1. Gondolkodj előre!

Minden, amit posztolsz, elmenthető - még ha eltűnik is utána.

🧠 Ne ossz meg túl sok személyes infót, például iskolát, otthonot, helyszínt vagy napi rutinokat!

2. Blokkolj és némíts = ez önvédelem

Ha valaki furcsa, gyűlölködő vagy csak idegesítő dolgokat küld — azonnal blokkold!

3. Zárd le a fiókjaidat

-Privát fiók = a te erőd: Állítsd be, hogy csak te dönts el, ki követhet. Használj arcfelismerést, ujjlenyomatot vagy PIN-kódot Windows-on: Beállítások → Fiókok → Bejelentkezési lehetőségek: jelszó után PIN, ujjlenyomat, arcfelismerés azonosítást kér.

-Kétfélepcsős azonosítás (2FA): Mindig kapcsold be. Ha valaki megszerzi a jelszavad, a második kód nélkül akkor sem tud belépni.

→ 2FA beállítása:

Windows: <https://account.microsoft.com/security> „További biztonsági beállítások” → „Kétfélepcsős azonosítás beállítása”

(telepíteni kell mobilra és Microsoft fiókkal jóváhagyni értesítéssel vagy kóddal).

Android: „Beállítások” → „Google” → „Biztonság” → „Kétfélepcsős azonosítás”

→ Választhatasz SMS-t, emailt vagy Authenticatort

-Használj jelszókezelőt! (pl. Bitwarden, 1Password)

4. Vigyázz az adathalász vagy kamu linkekkel

Kapsz egy üzenetet: „OMG, ez te vagy??” és egy link? 🚨 NE KATTINTS!

Ez általában csapda a fiókod ellopására.

🧠 Csak olyan linkekre kattints, amit megbízhatónak érzel. Ha gyanús, valószínűleg az is.

5. Mit tegyél, ha támadnak

Ne válaszolj. Pont ezt akarják.

Készíts képernyőfotót mindenről. A bizonyíték számít. Blokkolj és jelentsd be.

→ Képernyőkép készítés módja:

Windows: PrtScn (PrintScreen)

Android: Bekapcsoló Gomb + Hangerő le (gyártónként különbözhet)

→ Képek / Photos → képernyőképek / Screenshots

→ Jelentés módja:

Instagramon, TikTokon, X-en, Snapchaten stb.:

Koppints a profiljuk vagy posztjuk melletti három pontra (...)

Válaszd a „Jelentés” vagy „Felhasználó jelentése” lehetőséget

Kövessd az utasításokat!

🧠 Ha komoly (fenyegetés, zaklatás, zsarolás), szólj egy felnőttnek és jelentsd a helyi kiberbűnözés elleni hatóságoknak.

Okos jelszóhasználat tiniknek

„Bánj a jelszavaiddal úgy, mint a titkaiddal: legyen erős, egyedi, és NE osztd meg.”



1. KÉSZÍTS: Erős és okos jelszavakat

Használd ezt a képletet:

- Legalább 12 karakter
- Keverj nagy- és kisbetűket, számokat és jeleket
- Szavak átalakítása: á = a1, ő = o2, v. i = 1, v = 5,
- Ne használj személyes adatot (például neved, születési dátum, háziállat neve)

TIPP: Alakíts mondatot jelszóvá:

„A kutya este 7-kor ugat!” → AkEs7u!

2. KÜLÖNBÖZTESD MEG: Egy jelszó ≠ minden fiók

Soha ne használd ugyanazt a jelszót több appban vagy weboldalon.

Ha az egyiket feltörik, mind veszélyben lesz. Használj kis módosításokat, ha muszáj:

Instagram → Foto\$Insta2025!

Iskolai email → Tanul&Fejl2025!

🧠 Légy okosabb: használj különböző jelszavakat. Így, ha az egyik zárat feltörik, a többi biztonságban marad.

3. TÁROLD: Hol tartsd biztonságban

CSINÁLD:

Használj jelszókezelőt (pl. Bitwarden, 1Password vagy a böngésződ biztonságos tárolóját).

Csak akkor írd le papírra, ha zárt fiókban vagy privát jegyzetfüzetben van.

NE CSINÁLD:

Ne mentsd jegyzetbe vagy Word dokumentumba a telefonon vagy gépen.

Ne oszd meg üzenetben, csetben vagy képernyőfotón.

4. EMLÉKEZZ: Edzd az agyad

Használj mintákat, rímet vagy vizuális trükköket a fontos jelszavak megjegyzéséhez.

Példa: Iskolához: „Könyvek<3@” → Kép: 📚 + ❤️ + 🧠

Teszteld magad néhány hetente.

KEZELD: Tartsd titokban

A jelszavad olyan, mint a fogkeféd:

Csak te használd!

Cseréld le, ha régi, megosztott vagy kiszivárgott

Ne oszd meg a barátaiddal, még a legjobb barátokkal sem.

Ha muszáj megosztani (pl. családi Netflix), inkább külön fiókot vagy profilt hozz létre.

Bónusz tipp: Figyelj erre...

Jelszó kérés emailben vagy üzenetben = adathalászat

Furcsa kinézetű bejelentkezési oldalak = hamis webhelyek

Véletlenszerű felugró ablakok = kártevő csapdák

Ellenőrizd az URL-t (webcím) és kapcsolj be a kétfélszörös azonosítást (2FA), amikor lehet.

Néha ellenőriz - feltörték-e:

🔗 <https://haveibeenpwned.com/>

Az email cím beírásával megkaphatjuk, hogy feltörték-e.

Előzd meg a pszichológiai manipulációt!

„Ha valaki sürget, bűntudatot kelt vagy megfélemlít ... az csapda.”



A pszichológiai manipuláció akkor történik, amikor valaki megpróbál becsapni, hogy megadja neki a személyes adatokat, jelszavakat, vagy akár hozzáférést a fiókjaidhoz. Ez olyan, mint a digitális manipuláció. Nem az eszközt „törik fel”, hanem téged „törnek fel”.

Gyakori pszichológiai manipuláció trükkök:

Adathalászat: Hamis üzenetek vagy email-ek:

„OMG, te vagy ebben a videóban?”

„Kattints ide, hogy megkapd az ingyenes nyereményed!”

„Felfüggesztették a fiókodat, jelentkezz be most!”

Ismerősnek kiadva magukat:

Egy „barát”, aki jelszót kér.

Valaki, aki azt mondja: „Én vagyok az iskolai rendszergazda, beállíthatom újra a jelszavad?”

Érzelmi nyomás:

„Ha nem válaszolsz 5 percen belül, baj lesz.”

„Tiltásban leszel, ha nem kattintasz most!”

Így véd meg magad profi módon:

1. **Lassíts le! Mindig.**

Ha az üzenet sürgető, érzelmes vagy furcsa — állj meg és gondolkodj.

A csalók azt akarják, hogy gyorsan cselekedj gondolkodás nélkül.

Lassú = biztonságos. Gyors = kockázatos.

2. **Soha ne ossz meg személyes adatot**

Jelszavak, kódok, címek vagy iskolai infók nem mennek MS-en vagy SMS-ben - még „barátokkal” sem.

Ha valakinek tényleg segíteni kell, hívni fog vagy személyesen beszél veled.

3. **Ellenőrizd a forrást kétszer is**

Ha egy barát furcsa linket küld, kérdezd meg: „Tényleg te küldted ezt?”

Nézd meg az email címeket — például a support@instagram.com nem ugyanaz, mint az insta-help4421@gmail.com

4. **Használj kétfaktoros azonosítást (2FA)**

Még ha valaki meg is szerzi a jelszavadat, a második kód nélkül nem tud belépni, amit a telefonodra vagy emailre küldenek.

✓ **Ne szégyellj jelenteni**

Becsapott? Okos emberekkel is megtörténik.

Jelentsd a hamis üzeneteket a közösségi oldalakon (érintsd meg a ... > Jelentés)

Mondd el egy megbízható felnőttnek, tanárnak vagy iskolai rendszergazdának.

Hogyan gyorsíthatja fel az MI a kitétséget (és mit lehet ellene tenni)?

„Az MI képes hangokat másolni, hamis videókat készíteni és realisztikus csalásokat írni, de nem tudja helyettesíteni a kritikus gondolkodásodat. Az a valódi erő!”



Mi is az az MI?

Az MI (Mesterséges Intelligencia) olyan, mint egy szuper okos számítógépes agy. Ez működteti például:

- Csetbotokat
- Arcfelismerőket
- Okos asszisztenseket (mint Siri vagy Alexa)
- Sőt, még a TikTok „Neked” oldalát is

Az MI-t használhatják jó vagy rossz célokra is.

Hogyan használják a rosszfiúk az MI-t, hogy betörjenek vagy átverjenek téged

Okosabb csalások:

Az MI szuperrealisztikus üzeneteket tud írni, amik úgy hangzanak, mintha a barátaid, az iskolád vagy akár a szüleid írták volna.

Példa: „Szia, itt Szabó néni az iskolából — kattints ide a fiókod visszaállításához.”

Figyelem: hamis.

Hamis képek és videók (deepfake-ek)

Az MI képes hamis arcokat, hangokat (akár valós személyek hangját is utánozhatja!) vagy videókat készíteni, amik valósnak tűnnek — hogy megtéveessenek vagy kellemetlen helyzetbe hozzanak embereket.

Tömeges támadások

Az MI ezeket képes automatikusan adathalász e-maileket vagy üzeneteket küldeni, remélve, hogy valaki bedől nekik.

Csetbotok, amik embernek adják ki magukat

Lehet, hogy egy botnak beszélsz, nem embernek - és lehet, hogy azt tanították meg, hogyan csaljon ki tőled információkat.

Gondolkojd, mielőtt mindent elhiszel

Ha egy örült videót vagy sokkoló üzenetet látsz, ellenőrizd a tényeket.

Kérdezd meg: „Lehet, hogy ezt az MI készítette?”

Extra tipp: az MI segíthet neked is!

Az MI nem csak fenyegetés — védekezésre is használják:

- Spam szűrők az e-mailekben
- Arcfelismerő a telefonodon
- Gyanús belépések felismerése Instagramon vagy TikTokon

Netikett fiataloknak

„Az online tér olyan, mint egy digitális szomszédság”

Netikett fiataloknak

Védd a magánéleted!

Gondold át mit osztasz meg magadról.
Ha nem beszélnél róla hangosan egy teli szobában, akkor ne tedd ki sehova. Használd erős, egyedi jelszavakat és kétfaktoros azonosítást.

Gondolkozz mielőtt gépelsz!

Gondold át miket posztolsz, kommentelsz és osztasz meg. Mondanám ezt valakinek személyesen? Hogy érezném magam, ha rólam mondanák ezt? A törlés létezik, de a képernyőképek örökre megmaradnak!

Légy kedves. Légy tisztelettudó. Légy emberi.

Kerüld el az érzelmeid megosztását publikusan, beszélj inkább a barátalddal vagy megbízható felnőttekkel offline. Soha ne posztolj csak azért, hogy visszavágj másoknak. Minden ott marad online. Örökre.

Használd jóra a platformjaid!

Ossz meg inspiráló, felemelő, hasznos tartalmakat. Mások sikerét oszd meg, ne a rossz pillanataikat. A mentális egészség fontosabb, mint a folyamatos online jelenlét.

Nem kell a dráma!

Nem minden igaz, ami online megjelenik. Kerüld el a pletykák, álhírek terjesztését. Ha gyűlölködést látsz, jelentsd!

Ezeket kerüld el online:

Szólj egy felnőttnek, ha:

- nem érzed biztonságban magad online
- internetes zaklatást észlelsz.

Ne hasonlítsd az életed a másik profilján látható "tökéletességhez".

Szabj határokat és kapcsolódj ki!

Tarts szünetet netezés közben. Ne hídd el, hogy másoknak az az igazi életed, amit a netre kiraknak. Tarts közösségi média mentes időszakokat!

Ha rosszra fordulnak a dolgok - szólj róla!

Szólj egy megbízható felnőttnek - ha rosszul érzed magad, azonnal jelezd! Nem vagy egyedül!

1. Védd a magánéleted

Ne ossz meg személyes adatokat, mint a teljes neved, iskola, cím, telefonszám vagy napi rutinod. Használd erős, egyedi jelszavakat, és kapcsolódj be a kétfaktoros azonosítást (2FA).

Tartsd fiókjaidat privátnak, pontosan tartsd nyilván, kik láthatják a posztjaidat.

2. Gondolkozz, mielőtt gépelsz

Állj meg, mielőtt posztolsz, kommentelsz vagy megosztasz valamit. Kérdezd meg magadtól:

„Ezt megmondanám valakinek szemtől szembe?”

„Hogy érezném magam, ha rólam szólna?”

Kerüld a szarkazmust vagy a sötét vicceket — nem mindig úgy érti a másik, ahogy gondoldod.

A törlés gomb létezik, de a képernyőfotók maradnak.

3. Légy kedves. Légy tisztelettudó. Légy ember.

Kezeld másokat úgy, ahogy szeretnéd, hogy veled bánjanak — még online is.

Ne legyél troll. Ne tápláld a trollokat.

Állj ki másokért és jelentsd a zaklatást felnőttnek.

4. Használd jóra a platformjaid

Ossz meg inspiráló, felemelő vagy tanulságos tartalmakat. Ünnepezd mások sikereit. Támogasd a barátaidat. Ha gyűlöletet látsz, jelentsd. A hangod számít - használd bölcsen.

5. Nem kell a dráma

Kerüld az érzelmeid túlzott megosztását vagy a panaszkodást nyilvános fórumokon. Ha feldúlt vagy, beszélj egy megbízható baráttal vagy felnőttel személyesen. Ne írd homályos posztokat!

Ellenőrizd a forrásokat

Nem minden igaz az interneten. Kerüld a pletykák, álhírek vagy ijesztő „trendi” kamu sztorik terjesztését. Ha túl sokkolónak, viccesnek vagy drámainak hangzik - valószínűleg kamu.

6. Ezeket kerüld online

Kiberzaklatás (zaklatás, kizárás, személyiséglopás)
Ghosting (amikor valaki hirtelen, minden magyarázat nélkül megszakítja a kapcsolatot egy másik személlyel, szellemmé válik) indoklás nélkül
Spam (kéretlen vagy tömeges üzenet, amit általában e-mailben jönnek és kártékonyak)
 Nyilvános megszégyenítés vagy „beszólás”.

7. Szabj határokat és kapcsolódj ki

Nyugodtan kapcsolj ki és pihenj. Ne hasonlítsd magad mások csillogó életéhez. Használd képernyőidő-beállításokat vagy tarts szünetet a közösségi médiából.

8. Ha probléma van - szólj róla

Mondd el egy megbízható felnőttnek, ha: Nem érzed magad biztonságban, valaki fenyeget vagy zaklat, láttál vagy tapasztaltál zaklatást. Jelentsd a visszaélést az app beépített eszközeivel (Instagram, TikTok, Snapchat mind „Jelentés” opciót kínálnak)!

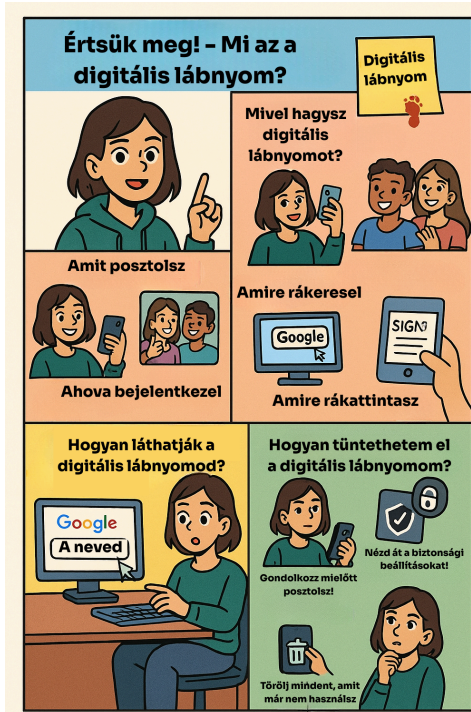
Kérj engedélyt mások képeinek posztolása előtt

Fogadd el, ha nemet mondanak.

Ne ossz meg ciki fotókat vagy videókat - még ha „csak viccnek” is számod.

Mi az a digitális lábnyom (és miért fontos)?

„A digitális lábnyomod olyan, mint egy tetoválás az interneten — győződj meg róla, hogy büszke vagy rá.”



Minden alkalommal, amikor online vagy — legyen az egy szelfi posztolása, egy videó lájkolása, valami keresése a Google-ben vagy Wi-Fi-re való belépés — apró nyomokat hagysz magad után. Ezeket a nyomokat digitális lábnyomodnak hívjuk. Olyan, mint amikor hóban sétálsz: minden lépés nyomot hagy. Csak itt az interneten történik, és akár örökre meg is maradhat.

Hogyan hagysz digitális lábnyomot (anélkül, hogy észrevennéd)?

Amit posztolsz: Fotók, videók, feliratok és kommentek, sztorik, bemutatkozások, felhasználónevek, hashtagek.
Amit mások posztolnak rólad: Csoportképek, amin be vagy jelölve, bejegyzések, amikben megemlítik a neved vagy az iskolád.
Amit keresel vagy amire kattintasz: Google keresések, kattintott linkek, videók.
Amire regisztrálsz: Közösségi média fiókok, online játékok, kvízek, nyereményjátékok, appok.

Hogyan láthatja valaki a digitális lábnyomodat?

Írd be a neved a Google-be — mi jelenik meg?

A barátaid, iskolák, sőt a jövőbeli munkahelyek is ezt teszik majd.

Hirdetések és cégek követik a kattintásaidat és lájkjaidat, hogy profilt készítenek rólad (mit szeretsz, mit veszel, mit nézel).

Az Internet NEM felejt - Nézz utána mit mentett el rólad:

- <https://web.archive.org/> - **Időgép**: mit mentett el (kapcsold be a fordítót!)
- <https://archive.ph/> - megőrzi a dinamikus oldalakat is
- <https://timetravel.mementoweb.org/> - archívum aggregátor: több helyen is keres

Hogyan tisztítsd (és kezeld) a digitális lábnyomod

1. Google-öld magad rendszeresen

Keressd a neved idézőjelek között: „A te neved” + város vagy iskola.

Ha valami furcsát találsz, kérd, hogy vegyék le.

2. Szigorítsd a privát beállításokat

Tedd a fiókjaidat priváttá. Csak a barátok lássák a posztjaidat. Kapcsold ki a helymeghatározó címkéket.

Próbáld ki: Instagram, TikTok, Google & YouTube → Beállítások → Adatvédelem

3. Töröld, amit már nem használsz

Régi fiókok? Zárd be őket. Nem használt appok? Töröld le őket. Furcsa posztok? Töröld.

4. Gondolkodj, mielőtt posztolsz

Kérdezd meg magadtól:

„Rendben lenne, ha a tanárom, a nagymamám vagy a jövőbeli főnököm látná ezt?”

5. Használj tisztább eszközöket

Használj adatvédelem-központú böngészőt (például DuckDuckGo: <https://duckduckgo.com/>)

Rendszeresen töröld a keresési és helymeghatározó adatokat

Használj jelszókezelőt, hogy csökkentsd a kockázatos bejelentkezéseket!

Hogyan szűrjük ki az álhíreket, deepfake-eket és dezinformációt – ELLENŐRízd!

„Ne hidd el, amit látsz — gondolkodj, mielőtt megosztod.”



Mi is az a dezinformáció?

Dezinformáció = szándékosan terjesztett hamis információ, amely célja, hogy összezavarjon, megtéveessen vagy megosszon embereket.

Ez megjelenhet például:

- Hamis hírek
- Deepfake videók vagy hamisított hangfelvételek (MI által szerkesztett)
- Manipulált fotók
- Vírusos posztok vagy mémek, amelyek kitalált tényeket tartalmaznak

HA MÉGIS MEGOSZTOTTA – MIT TEGYÉL:

- Töröld amint lehet!
- Frissítsd a posztot megírva, hogy kamu a hír!

Ellenőrizd a forrást

Létező és megbízható forrásra hivatkozik?

Lejárt a dátum?

Ellenőrizd hitelesítő eszközökkel

Nagyíts rá a képekre és videókra

Őrizd meg a nyugalmad és olvasd tovább a címsoron túl

Reális, hihető tartalom?

Ne oszd meg, amíg nem *ELLENŐR*-izted!

További részletek találhatóak az E. mellékletben!

Miért kell megjelölni az MI által generált tartalmakat - mit tegyél, ha hiányzik a jelzés?

„Ha tudod, mi valós, könnyebben tudsz saját magadért gondolkodni.”



Mi az az MI által generált tartalom?

Az MI által generált tartalom olyan fotókat, videókat, hangfelvételeket vagy szövegeket jelent, amelyeket mesterséges intelligencia hozott létre vagy szerkesztett, nem pedig valós események.

Néhány példa:

- Egy hírességről készült videó, amiben olyasmit mond, amit soha nem mondott
- Egy tüntetésről készült fotó, ami valójában soha nem történt meg
- Egy „hangüzenet”, ami úgy szól, mintha a tanárod lenne, de valójában egy bot készítette

Miért kell ezt felcímkézni

Az Európai Unió, megköveteli, hogy az MI által készített tartalmakat egyértelműen jelöljék a következő fontos okok miatt:

1. Az igazság védelme érdekében

Címkék nélkül az emberek nem tudják megkülönböztetni, mi valódi és mi hamis.

A deepfake-eket hazugságra, csalásra vagy bántásra lehet használni.

A címkézés segít eldönteni, miben hihetsz.

2. A manipuláció megelőzése érdekében

Az MI hamis történeteket terjeszthet választások, háborúk vagy vészhelyzetek idején.

A címkék megállítják a pánikot, félelmet vagy tisztességtelen befolyásolást.

A te véleményed számít - ne hagyd, hogy egy hamis videó alakítsa.

3. A bizalom építése érdekében

A művészek, influencers és márkák, akik jelölik az MI használatát, őszinték.

Ez megmutatja, hogy nem akarnak megtéveszteni senkit.

Őszinteség az interneten = biztonságosabb net mindenkinek.



Mit tegyél, ha nem jelölt MI tartalmat találsz?

1. Állj meg megosztás előtt és gondolkodj!
Ha túl sokkolónak, drámáinak vagy furcsának tűnik - még ne oszd meg.
2. **ELLENŐR**-izd le kétszer is!
3. Jelentsd: TikTokon, YouTube-on, Instagramon vagy X-en (Twitter):
Koppints a három pontra (...) a poszton
Válaszd a „Jelentés” opciót
Válassz olyasmit, hogy „Megtévesztő vagy manipulált média”
Nem árulkodsz - az igazságot véded.

Hogyan segítheti az MI a negatív információk terjedését

„Nem minden arany, ami fénylik!”



Algoritmikus felerősítés: Az a mód, ahogy a közösségi média platformok algoritmusai növelik bizonyos tartalmak láthatóságát — néha akaratlanul is elősegítve a dezinformáció terjedését.

Példa: Senszációhajhász vagy félrevezető posztok vírusossá válása az elköteleződésre fókuszáló algoritmusok miatt.

Visszhangkamra: Olyan online környezet, ahol az emberek csak olyan véleményekkel találkoznak, amelyek megerősítik a sajátjait, korlátozva a kritikai gondolkodást.

Példa: Egy közösségi média hírfolyam, amely csak egy politikai nézőpontot mutat be.

Megerősítési torzítás: Az a hajlam, hogy olyan információkat higgyünk el vagy osszunk meg, amelyek megerősítik meglévő nézeteinket, függetlenül azok valóságtartalmáról.

Példa: Hiteles források figyelmen kívül hagyása, amelyek ellentmondanak a kedvelt véleménynek.

A negatív információ fajtái:

- **Dezinformáció:** Szándékosan hamis információ, amelyet arra hoznak létre és terjesztenek, hogy megtéveszsenek vagy félrevezessenek embereket.
Példa: Hamis hírek, amelyek célja a közvélemény manipulálása.
- **Félreinformál:** Hamis vagy pontatlan információ, amelyet nem szándékosan osztanak meg félrevezetés céljából.
Példa: Egy rosszul feliratozott kép megosztása úgy, hogy azt igaznak hiszik.
- **Káros információ:** Valódi információ, amelyet azért használnak, hogy kárt okozunk egy személynek, szervezetnek vagy országnak.
Példa: Bizalmas adatok kiszivároztatása valaki megszégyenítésére.
- **Álhír:** Kitalált hírek, amelyeket legitim újságíróként mutatnak be, gyakran a közösségi médiában terjednek.
Példa: Vírusos címlapok, amelyek hamis tudományos felfedezéseket állítanak.
- **„Deepfake”:** Szintetikus média (általában videó vagy hang), amelyet MI generál, hogy valós embereket imitáljunk, gyakran meggyőző módon.
Példa: Egy videó, amelyen egy politikus szájába adnak szöveget
- **Gyűlöletbeszéd:** Olyan beszéd, írás vagy tartalom, amely egy személyt vagy csoportot faji, vallási, etnikai, politikai, nemi, szexuális irányultság vagy más identitás alapján gyűlölettel vagy erőszakra uszítással támad.
Példa: „Az összes [etnikai csoport] csak bajt hoz ránk!”
- **Trollkodás:** Szándékosan provokatív, bántó vagy félrevezető kommentelés az online térben, azért, hogy érzelmi reakciót váltson ki vagy vitát gerjeszt.
Példa: Valaki egy természetvédelmi poszt alá azt írja: „Remélem, kivágják a fákat!”
- **Kattintásvadász tartalom:** Olyan megtévesztő vagy túldramatizált cím, amely arra készíti az olvasót, hogy rákattintson – pedig a tartalom más mint, amit a cím ígér.
Példa: „Sokkoló mit tett a kedvenc színészed – nem fogsz hinni a szemednek!”
(A cikkből pedig kiderül, hogy csak interjút adott.)

MI: A menő és a kínos

„Az MI olyan, mint a tűz: megfőzheti a vacsorád, vagy felgyújthatja a házat.”



✓ A jó dolgok amire az MI képes

1. Segít menő dolgokat alkotni

Az MI eszközök segíthetnek írni, rajzolni, videókat szerkeszteni vagy zenét készíteni.
Példa: Adsz neki egy ötletet, és ő művészetet vagy rövid történetet alkot belőle.
Olyan, mintha lenne egy kreatív asszisztens, aki mindig elérhető, éjjel-nappal.

2. Fokozza a tanulásodat

Az MI különböző módokon magyaráz el dolgokat (mint például a ChatGPT).

Segíthet matekból, fordításban, vagy kvízeket csinálhat a vizsgára való felkészüléshez.

Nem helyettesíti az agyadat, de támogatja azt!

3. Inkluzívabbá teszi az életet

Beszédből szöveg funkció azoknak, akik nem tudnak gépelni. Eszközök, amelyek leírják a képeket vakoknak. Fordító eszközök, amelyek bontják a nyelvi korlátokat. Segít az embereknek kapcsolódni, még ha eltérő igényeik vagy nyelvük van is.

4. Védelmet nyújt online

Kiszűri a spamet és csaló emaileket.

Figyeli a zaklatást vagy gyűlöletbeszédet a platformokon.

Felismeri a hamis fiókokat és gyanús tevékenységet.

Néhány MI a háttérben dolgozik, hogy biztonságosabbá tegye az internetet.

⚠ A nem olyan jó dolgok amire az MI képes

1. Hamis információk terjesztése

Az MI képes deepfake videókat, hamis képeket és hamis hangokat készíteni.

Hamis híreket írhat vagy kitalált tényeket állíthat be úgy, hogy hihetőnek tűnjenek.

Csak mert valami valósnak látszik, még nem biztos, hogy igaz is.

2. Gondolkodás helyettesítése

Ha mindent az MI-re bízol (például hogy írja meg az esszédet), akkor abbahagyod a saját gondolkodást. Így lemaradsz a tanulásról és fejlődésről.

3. Elfogultság beépítése

Az MI az adatokból tanul. Ha az adatok elfogultak (például rasszizmus vagy sztereotípiák), az MI ezt megismételheti. Igazságtalan eredményeket adhat vagy kirekeszthet embereket. Az MI nem tökéletes, azokat tükrözi, akik létrehozták.

4. Követés és adatvédelem

Néhány MI eszköz követi, hogy mit keresel, hogy megismerje a szokásaidat.

Aztán még több hasonló tartalmat mutat — még ha nem is jó neked.

Ezért fontos az alkalmazás beállításait elolvasni és kontrollálni az adataidat.

Miért lehet az MI túlhasználata veszélyes a tanulókra? Hogyan akadályozzuk meg?

„Az MI menő. Az elméd még menőbb. Használd mindkettőt — de az agyad vezessen.”



Az MI hihetetlen dolgokra képes:

- Esszéket ír
- Matekpéldákat old meg
- Tudományos fogalmakat magyaráz
- Még műalkotásokat is generál

De itt a lényeg: ha hagyod, hogy mindent helyetted csináljon, lassan kezd helyettesíteni a saját gondolkodásodat — és itt kezdődik a veszély.

Mi történik, ha túl sokat használsz az MI-t?

1. Az agyad lustul

Ha az MI old meg minden problémát helyetted, nem gyakorolod a gondolkodást.

Ha kihagyod az edzést, az izmok gyengülnek — ha nem használod az agyad, az is gyengül.

2. Elveszíted a saját hangodat

Az MI sablonos, udvarias stílusban ír — de az nem te vagy. A személyiséged nem jön át.

3. Kevesebbet tanulsz, még ha „gyorsabban

kész is vagy” — de másnapra elfelejted.

✓ Hogyan használd az MI-t bölcsen (anélkül, hogy helyettesítsen)

1. Használd az MI-t támogatásra, ne helyettesítésre

Kérd meg, hogy magyarázzon el egy fogalmat, adjon példákat vagy foglaljon össze valamit. Aztán használd a saját szavaidat és ötleteidet a válaszhoz vagy íráshoz. Gondolj rá úgy, mint egy tanuló társra, nem egy helyettes agyra.

2. Először a saját gondolataiddal kezdj

Gondolkodj el, mielőtt az MI-hez fordulsz segítségért.
Majd hasonlítsd össze az ötleteket és erősítsd meg a sajátodat.
Ne veszítsd el a saját hangodat. Egészítsd ki azt.

3. Tanuld meg felismerni az MI-stílust

Az MI hasznos, de gyakran túl formális vagy homályos.
Írás közben mindig ellenőrizd:
„Ez engem tükröz?”
„Egyetértek ezzel a válasszal?”

4. Tarts egyensúlyt

Állíts fel szabályokat magadnak:

- ✓ Használd az MI-t átnézéshez vagy visszajelzéshez
- ⊘ Ne hagyd, hogy teljesen helyetted írjon esszét

Az egyensúly = a képességeid fejlesztése és az eszközök okos használata.

TANULJ MI-vel – 10 okos módon

„Az MI arra való, hogy tágítsa a gondolkodásodat – nem arra, hogy helyettesítsd!”

TANULJ MI-vel – 10 okos módon

„Az MI arra való, hogy tágítsa a gondolkodásodat – nem arra, hogy helyettesítsd!”

T – Tervezz előre!

Mielőtt kérdeznél az MI-től, gondold át, mit tudsz már a témáról, és mit szeretnél megtudni. Ez segít, hogy a saját gondolataid vezessenek, ne a gép.

A – Alakítsd saját szavaiddal!

Ne másold le, amit az MI ír – fogalmazd meg újra, hogy valóban megérted.

N – Ne hidd el azonnal!

Az MI néha téved. Ellenőrizd a válaszokat megbízható forrásokban vagy a tanárral.

U – Utánajárással erősítsd meg!

Kérdezz vissza: „Miért így van?”, „Hogyan működik ez a folyamat?”
A megértés mélysége a kérdésekből fakad.

L – Légy kreatív!

Használd az MI-t ötletelésre, példák keresésére, vagy új nézőpontok felfedezésére – de te dönts el, mit tartasz jónak.

J – Jegyezd meg, amit tanultál!

Írd le a saját szavaiddal, amit az MI segítségével megértettél.
A tudás akkor lesz a tiéd, ha te magyarázni is tudod.

M – Mérlegeld a forrásokat!

Gondold végig, honnan származik az információ.
Ne csak az MI-ben bíz, hanem a logikában is.

I – Ismerd meg, hogyan működik!

Az MI nem tud, csak mintákat jósol.
Ha megérted, hogyan gondolkodik, tudni fogod, hogyan segíthet neked.

V – Védj a személyes adataidat!

Soha ne ossz meg személyes vagy iskolai információt.
A biztonság is a felelős tanulás része.

E – Engedd a kihívásnak!

Az MI lehet edző, nem pedig helyettes. Kérd, hogy magyarázza el másképp, vagy kérdezz vissza – így fejlődsz igazán.

L – Légy te a pilóta!

Az MI a segítő, te irányítasz.
Használd arra, hogy mélyebben értsd meg a világot – ne arra, hogy megspórolj a gondolkodást.

T – Tervezz előre!

Mielőtt kérdeznél az MI-től, gondold át, mit tudsz már a témáról, és mit szeretnél megtudni. Ez segít, hogy a saját gondolataid vezessenek, ne a gép. Ha előre meghatározod a kérdéseidet, tudatosabb leszel, és könnyebben felismered, hogy az MI válasza valóban hasznos-e.

A – Alakítsd saját szavaiddal!

Ne másold le, amit az MI ír – fogalmazd meg újra, hogy valóban megérted. A tanulás akkor történik meg, ha az információt a saját gondolkodásodon „átszűrve” újraalkotod.

N – Ne hidd el azonnal!

Az MI néha téved. Ellenőrizd a válaszokat megbízható forrásokban vagy a tanárral. Az MI nem tényeket tud, hanem mintákat követ, ezért hibázhat.

U – Utánajárással erősítsd meg!

Kérdezz vissza: „Miért így van?”, „Hogyan működik ez a folyamat?” A megértés mélysége a kérdésekből fakad. A kritikus gondolkodás alapja, hogy ne csak elfogadj, hanem megérted az összefüggéseket.

L – Légy kreatív!

Használd az MI-t ötletelésre, példák keresésére, vagy új nézőpontok felfedezésére – de te dönts el, mit tartasz jónak. Az MI rengeteg ötletet adhat, de az értékes gondolatok kiválasztása mindig az ember feladata.

J – Jegyezd meg, amit tanultál!

Írd le a saját szavaiddal, amit az MI segítségével megértettél. Az aktív ismétlés és újrafogalmazás rögzíti az ismereteket a hosszú távú memóriában.

M – Mérlegeld a forrásokat!

Gondold végig, honnan származik az információ. Ne csak az MI-ben bíz, hanem a logikában is. A digitális világban nem minden információ hiteles, az MI pedig gyakran nem jelzi, honnan vette az adatot.

I – Ismerd meg, hogyan működik!

Az MI nem tud, csak mintákat jósol. Ha megérted, hogyan gondolkodik, tudni fogod, hogyan segíthet neked. Ha tisztában vagy az MI korlátaival, okosabban használod, és elkerülsz a félreértéseket.

V – Védj a személyes adataidat!

Soha ne ossz meg személyes vagy iskolai információt. A biztonság is a felelős tanulás része. Az interneten megosztott adatok tartósan megmaradhatnak, és visszaélhetnek velük.

E – Engedd a kihívásnak!

Az MI lehet edző, nem pedig helyettes. Kérd, hogy magyarázza el másképp, vagy kérdezz vissza – így fejlődsz igazán. A kihívás gondolkodásra ösztönöz, és segít mélyebb szinten megérteni a tananyagot.

L – Légy te a pilóta!

Az MI a segítő, te irányítasz. Használd arra, hogy mélyebben értsd meg a világot – ne arra, hogy megspórolj a gondolkodást. Az önálló gondolkodás és döntéshozatal fejleszti a kritikai és kreatív képességeket.

Készítette az ELTE DRONE csapata 2025 október (v.2025.10.24):

- Dr. Turcsányi-Szabó Márta, habilitált egyetemi docens (tszmarta@inf.elte.hu), az ELTE Informatikai Kar oktatási innovációért felelős dékáni biztosa
- Mikófalvy Franciska, pedagógus, az ELTE IK T@T Kuckó koordinátora

MJ: Az ötleteléshez és a képek generálásához felhasználtuk a ChatGPT 5.0-t.

Jogi nyilatkozat

Az Európai Unió finanszírozásával készült. A közölt nézetek és vélemények kizárólag a szerző(k) álláspontját tükrözik, és nem feltétlenül egyeznek az Európai Unió vagy az Európai Oktatási és Kulturális Végrehajtó Ügynökség (EACEA) hivatalos álláspontjával. Az Európai Unió és az EACEA nem tehetők felelőssé ezért a tartalomért.

Szerzői jogi nyilatkozat



CC BY-NC 4.0



BY: Az alkotót meg kell nevezni.



NC: A mű kizárólag nem kereskedelmi célú felhasználása engedélyezett.



A „nem kereskedelmi célú” felhasználás azt jelenti, hogy az nem elsősorban kereskedelmi haszonszerzésre vagy anyagi ellenszolgáltatásra irányul.

Ez a mű a Creative Commons: Nevezd meg! – Ne add el! 4.0 Nemzetközi licenc feltételei szerint van licencelve.

Ez a licenc előírja, hogy a felhasználók megfelelő módon hivatkozzanak az alkotóra, és lehetővé teszi az anyag terjesztését, feldolgozását, átdolgozását és továbbfejlesztését bármilyen formátumban vagy médiumban, kizárólag nem kereskedelmi célokra.



**Co-funded by
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.