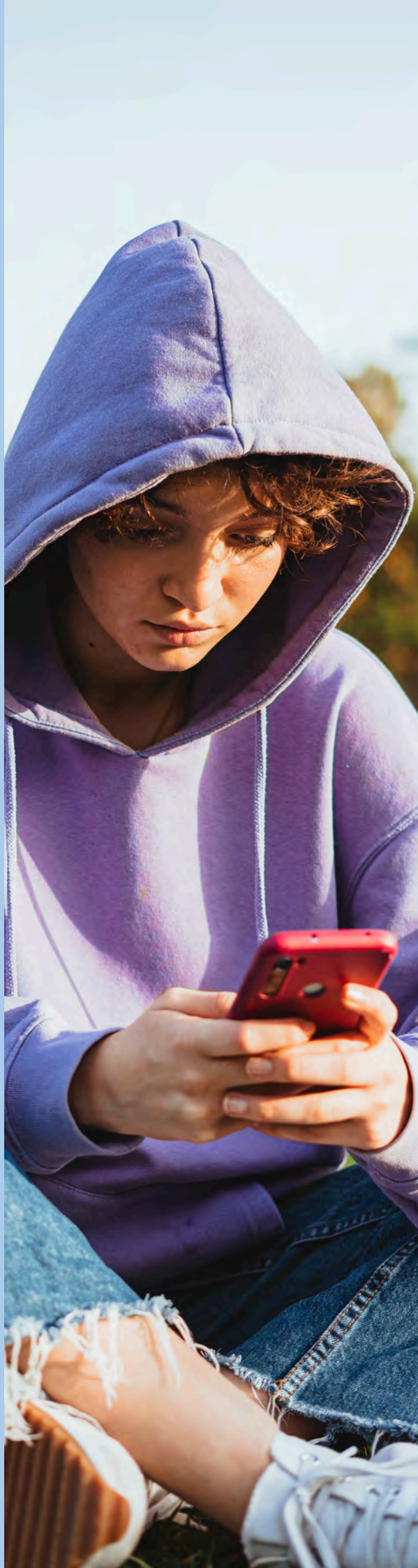
INHOPE | NMHH National Media and Infocommunications Authority • Hungary

Együtt erősebbek vagyunk- Útmutató a digitális műveltséghez

A magyar kiadást az Internet Hotline készítette.

Szerzők: A. Sotiri, Marketing Communications Officer and A. Dyka, Marketing Content Specialist, September 2024

Az Európai Unió támogatásával



Tartalomjegyzék

Miért van szükség digitális műveltségre?

A technológia folyamatosan változik, és gyorsabban alakul át, mint egy TikTok-trend. Lehet, hogy valaki profi az interneten, de legyünk reálisak: az online világban való biztonságos eligazodás nem csak az alkalmazások ismeretéről szól. Egy olyan online tér kialakításáról van szó, ahol a felhasználó biztonságban érezheti magát, ahol kapcsolatba léphet másokkal, és ahol mások tiszteletben tartják őt.

Tudjuk, hogy sokan és sokat beszélnek az „online biztonságról", de ez túlmutat azon, hogy kerüljük a gyanúsnak tűnő linkeket, vagy állítsunk be erős jelszót. Arról van szó, hogy megértsük, hogyan védhetjük meg magunkat, és figyeljünk arra, milyen interakcióba lépünk másokkal az interneten. Mi lenne, ha azt mondanánk, hogy a digitális műveltség nemcsak biztonságosabbá, hanem sokkal pozitívabbá és élvezetesebbé is teheti az interneten töltött időt a számodra és a környezetedben élők számára?

Ezért összeállítottunk néhány egyszerű, de hatékony tippet. Pár perc alatt megtanulhatod, hogyan kerüld el az átveréseket és az álhíreket, hogyan ismerd fel a veszélyt, és hogyan teremts olyan online teret, ahol te és a barátaid aggályok nélkül boldogulhattok. Miért számít ez? Mert az internet hatalmas, és az online kockázatokkal szemben nem létezik teljes körű védelem. Minél többet tudsz, annál jobb döntéseket hozhatsz a saját és mások biztonsága érdekében.

Ne felejtsd el, hogy még akkor is, ha minden szükséges lépést megtettél saját védelmed érdekében, akkor is előfordulhat, hogy valaki kihasznál – legyen szó akár ismerősről, akár idegenről. És ha valaki átlép egy határt, az mindig az ő hibája, és soha nem a tiéd. Megérdemled, hogy biztonságban érezd magad, és azt is tudnod kell, hogy mindig van elérhető segítség.

1. SZAKASZ

Ismered az eszközödet?

Az otthonodhoz vagy a szobádhoz hasonlóan a telefonod is a te személyes tered, ezért őrizd meg a biztonságát. De nem csupán arról van szó, hogy védd magad az ismeretlenekkel szemben, hiszen esetenként az ismerőseid, például a barátaid is átléphetik a határt, ha az engedélyed nélkül hozzáférnek a telefonodhoz vagy a személyes adataidhoz. A készülékedet érintő fenyegetésekkel szemben hogyan gondoskodhatsz adataid és magánügyeid biztonságáról? Kezdésként arra figyelj, hogy a lehető legtöbbet hozd ki az adatvédelmi és biztonsági funkciókból, hogy felügyelni tudd, ki férhet hozzá a személyes teredhez, mind az online, mind az offline térben.

Rendszeresen frissíted a telefonodat?

A szoftverfrissítések nagyon fontosak az online és offline biztonságod védelmében. Ezek általában korrigálják a korábbi verziókban észlelt sérülékenységeket, és gondoskodnak az eszköz legújabb biztonsági védelméről. A kiberbűnözők gyorsan kihasználják a rendszer gyenge pontjait, ezért a szoftverfrissítés segít megvédeni a készülékedet attól, hogy illetéktelenek hozzáférjenek, és potenciális fenyegetésnek tegyenek ki.

Milyen az erős jelszó?

A jelszó az első védelmi vonalad, tehát erősnek kell lennie. Ne használd a születési dátumodat vagy egyéb, hozzád tartozó személyes információkat, vagy olyan könnyen kitalálható kombinációkat, mint a „jelszó123". Legyenek a jelszóban számok, betűk és szimbólumok vegyesen, és legyen legalább 12 karakter hosszúságú. Minden fiókhoz más jelszót használj, és törekedj a kiszámíthatatlanságra. A védelem egy újabb rétegének hozzáadásához használj többfaktoros hitelesítést az összes online fiókodban, e-mailben és a közösségi médiában, hogy az adataid még akkor is biztonságban legyenek, ha valaki hozzáfér a jelszavadhoz.

Ki tudhatja, hogy hol jársz?

A készüléked képes nyomon követni, hogy hol vagy éppen, és a tartózkodási hely megosztása akár hasznos is lehet a tájékozódáshoz vagy a családdal való kapcsolattartáshoz. Fontos azonban, hogy alaposan gondold meg, mielőtt a tartózkodási helyedet megosztanád a barátaiddal vagy egy ismerősöddel. Ez ugyanis esetenként kontrolláló vagy akár bántalmazó viselkedéssé fajulhat. A folyamatos helymegosztás olyan helyzetet idézhet elő, amelyben valaki minden mozdulatodat figyeli, ami negatív hatással lehet a kapcsolataidra és a személyes biztonságodra.

Ha meg akarod védeni magad, a „Beállítások"-nál keresd meg a „Helymeghatározás" opciót, és válaszd ki, mely alkalmazások férhetnek hozzá a pozíciódhoz. Javasoljuk, hogy csak akkor engedélyezd az alkalmazásoknak, hogy kövessenek, amikor aktívan használod őket, alapvetően pedig korlátozd a tartózkodási hely megosztását, hogy megőrizd a személyes tered.

Lehallgat a telefonod?

Előfordulhat, hogy a készüléked ráhangolódik a környezeti hangokra. Miközben a zene, a podcastok hallgatása vagy a hangalapú utasítások használata fokozhatja a felhasználói élményt, mindenképpen szabályoznod kell, hogy ki hallgat téged. A készülék „Beállítások" menüjében a „Hang" vagy a „Mikrofon" menüpontban válaszd ki, hogy mely alkalmazások férhetnek hozzá a készüléked mikrofonjához. Szelektálj az engedélyek megadása során, és csak akkor engedélyezd az alkalmazásoknak, hogy hallgassanak, ha aktívan használod azokat. Így megbizonyosodhatsz arról, hogy a telefonod nem „hallgatózik" olyankor, amikor a legkevésbé sem számítasz rá.

Biztonságos a telefonod kamerája?

Az alkalmazások sok esetben engedélyt kérnek ahhoz, hogy hozzáférjenek a kamerához vagy a képgalériához, miközben használod őket. Bár egyes alkalmazásoknak szükségük van ezekre az engedélyekre a működéshez, például a képek megosztásához, másoknak azonban nincs. Ha gyanús alkalmazásoknak adsz hozzáférési engedélyt a kamerához, az ahhoz vezethet, hogy a személyes adataid illetéktelenek kezébe kerülnek, vagy akár a készüléked kamerájával is kémkedhetnek utánad. Ezt úgy előzheted meg, hogy korlátozod a hozzáféréssel rendelkező alkalmazások számát. Fontos, hogy elővigyázatos légy a hozzáférési engedélyek megadásakor, és alaposan gondold át, mielőtt bármilyen alkalmazást telepítesz. Mindig helyezd előtérbe az adatvédelmet és a biztonságot, és tartsd ellenőrzés alatt, hogy ki férhet hozzá a személyes adataidhoz.

Honnan lehet tudni, hogy mely alkalmazások biztonságosak?

Nem minden online alkalmazás biztonságos, némelyikük éppen az adataidra vadászik. Letöltés előtt mindenképpen nézd meg az alkalmazás értékeléseit az App Store-ban (iOS) vagy a Google Playen (Android). Mit mondanak róla az emberek? Van bármilyen figyelmeztető jel, amelyről tudnod kell? Ha pozitívak a visszajelzések, akkor nem kell aggódnod! Ha viszont valami gyanúsnak tűnik, bízz a megérzéseidben!

Ki férhet hozzá a közösségimédia-fiókodhoz?

Akárcsak a való életben, itt is te szabod meg, hogy ki tartozik a baráti köródbe, és ki férhet hozzá a személyes adataidhoz. A fiókjaid a tieid, és te döntöd el, hogy kit engedsz be, és kit nem. A legtöbb platform lehetővé teszi, hogy konkrét listákat hozz létre azokról az emberekről, akik láthatják a posztjaidat, ezért a privát információkat és képeket tartsd meg a belső kör számára, és ügyelj arra, hogy milyen tartalmakat osztasz meg a széles nyilvánossággal. Ha szeretnéd, hogy a fiókod nyilvános maradjon, alaposan gondold át, hogy mit teszel közzé, és kerüld az olyan személyes adatok közzétételét, mint a lakcím, a pénzügyi adatok vagy a lakóhely.

Hogyan böngészhetsz biztonságosan?

Mindig győződj meg róla, hogy az internet biztonságos felületein maradsz. Hogyan? Először is ellenőrizd a beállításaidat, és vizsgáld meg a biztonságodat szolgáló védelmi rendszereket. A népszerű böngészők fokozott védelmet kínálnak, és figyelmeztetnek, ha veszélyes webhelyeket vagy bővítményeket szeretnél megnyitni. Ha viszont még magasabb szintre szeretnél lépni a biztonságos böngészésben, érdemes megfontolni az adatvédelmi szempontú böngészők, például a DuckDuckGo vagy a Qwant használatát. Ezeket a böngészőket kifejezetten úgy tervezték, hogy védjék a személyes adataidat és az egyéb információidat az interneten.

Mindig győződj meg róla, hogy az internetkapcsolatod titkosított és biztonságos, és ellenőrizd, hogy a címsorban szerepel-e a „HTTPS". Ha a weboldal URL-címe nem „HTTPS"-sel kezdődik, jól gondold meg, hogy akarod-e használni. Főként, ha személyes adatot osztanál meg magadról, vagy megadnád a jelszavadat.

JÓ TANÁCSOK

A szüleid nem tudják eldönteni, hogy megkaphatod-e az első telefonodat? Megmutatjuk, hogyan tudod figyelembe venni az aggályaikat, miközben a privát szférád megóvását is szem előtt tartod.

Vannak olyan alkalmazások és eszközök, amelyek javíthatják az online élményt amellett, hogy óvják a biztonságodat és a magánéletedet. Ezek az eszközök segíthetnek abban, hogy közted és a szüleid között kialakuljon a bizalom, de az is fontos, hogy egészséges, számodra megfelelő digitális szokásokat alakíts ki, mindezt attól függetlenül is, hogy van-e otthon ilyen jellegű támogató segítséged vagy nincsen.

Egyes alkalmazások, mint például a Qustodio, olyan funkciókat kínálnak, mint a 'Biztonságos keresés', amely segít kiszűrni a zavaró tartalmakat, vagy a 'Pánik gomb', amellyel vészhelyzetben értesíteni tudsz egy olyan ismerőst, akiben megbízol. Ha a szüleidhez valami miatt nem tudsz fordulni, gondold át, van-e a környezetedben olyan felnőtt, akiben megbízol – lehet ez a személy egy másik családtag vagy akár egy tanár –, akihez segítségért fordulhatsz abban az esetben, ha valami zavaró dolgot tapasztalsz az interneten. Minden helyzetben a biztonságod a legfontosabb, és azt is tudd, hogy mindig van – akár a szüleidtől függetlenül is – elérhető segítség.

2. SZAKASZ

Kapcsolattartás az online térben

Tudsz-e változást elérni az interneten?

Az online interakció ugyanolyan fontos lehet, mint a személyes beszélgetés. Különösen, ha arról van szó, hogy milyen érzéseket vált ki belőlünk. A tiszteletteljes kommunikáció pozitív környezetet és erős online közösséget teremt. Ügyelj arra, hogy online kommentelés vagy csevegés közben is kedves legyél. Ha feldúlt vagy dühös vagy, pár percre szakadj el a telefontól vagy a laptoptól, és próbálj meg megnyugodni. Mielőtt rányomnál a küldés gombra, mindig gondolkozz el azon, hogy a szavaid milyen hatással lehetnek másokra. Ha bántó, sértő dolgot írnál, mérlegeld, hogy ugyanezt szemtől szemben is kimondanád-e.

Ugyanennyire fontos az is, hogy kiállj másokért. Ha szemtanúja vagy annak, hogy valakit zaklatnak, sértegetnek vagy bántalmaznak, jelentsd!

Miért kell átgondolnod, hogy mit osztasz meg másokkal online?

Minden online megosztásnak tartós nyoma marad, ezért egy pillanatig gondolkozz el, mielőtt megnyomnád a megosztás gombot. Tedd fel magadnak a kérdést: ez a tartalom tiszteletteljes, pontos, és olyan, aminek a megosztására engedélyt kaptam? A téves információk megosztása árthat másoknak, tönkreteheti a hírnevüket, vagy akár jogi következményekkel is járhat. A közösségi média algoritmusai gyakran felerősítik az ellentmondásos vagy szenzációhajhász tartalmakat, ami azt jelenti, hogy a félretájékoztatás gyorsan és széles körben terjedhet. Érdemes tehát kétszer is ellenőrizni a tényeket olyan megbízható eszközökkel, mint a Snopes, a FactCheck.org vagy a GoogleFactCheck. Ha valami túl extrémnek vagy túl szépnek hangzik ahhoz, hogy igaz legyen, valószínűleg szükséges ellenőrizni a tényeket.

A saját magánszférád és a biztonságod érdekében mindig légy óvatos azzal, hogy mit osztasz meg. Ha pedig másokról van szó, a lényeg a beleegyezés, különösen érzékeny helyzetekben. Mielőtt képet vagy információt teszel ki valakiről, kérdezd meg, hogy ez számára rendben van-e, és tartsd tiszteletben a döntését, bármi legyen is az. Ha véletlenül téves információt vagy káros tartalmat osztasz meg, cselekedj gyorsan, töröld, és hozd helyre a dolgokat. Ha odafigyelsz arra, hogy mit osztasz meg, segíthetsz biztonságosabbá és megbízhatóbbá tenni az online teret mindenki számára.

Hogyan lehet biztonságosan használni az MI-t?

A mesterséges intelligencia parancsra képes képeket, videókat, történeteket vagy hangüzeneteket generálni. Az ilyen eszközök kreatív használata szórakoztató lehet, de erőszakos, sértő vagy törvénybe ütköző anyagokat létrehozni helytelen dolog, és akár jogi következményekkel is járhat. Az MI felhasználható például arra, hogy olyan deepfake videókat hozzunk létre, amelyek megtévesztő módon ábrázolnak embereket azáltal, hogy olyan dolgokat tesznek vagy mondanak, amelyeket a valóságban soha nem tennének vagy mondanának.

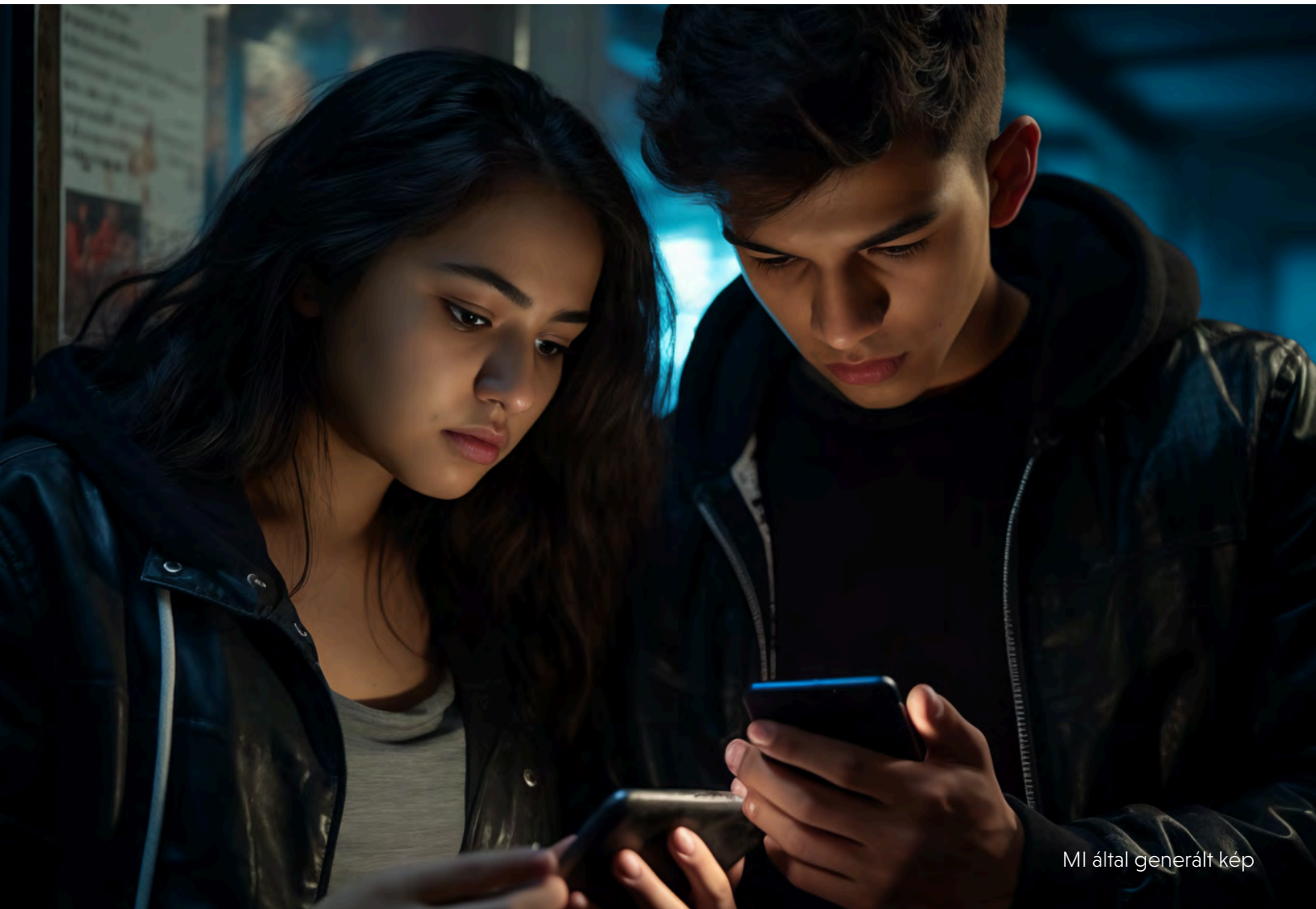
Ezek a deepfake tartalmak becsaphatják az embereket, zavart kelthetnek, és akár tartósan is árthatnak a jó hírnévnek vagy szétzúzhatnak kapcsolatokat. Ezért a saját érdekedben és másokra való tekintettel se hozz létre és ne terjessz semmilyen káros, MI által generált tartalmat. Mindig gondolj arra, hogy a hamis tartalomnak nagyon is valóságos hatása lehet.

Ma már bárki hozzáférhet az MI-eszközökhöz. Lehet, hogy használtad is már ezeket képgenerálásra, vagy segített az iskolai feladataid megoldásában, azonban ezekkel az eszközökkel visszaélni is sokféleképpen lehet.

Hogyan lehet arra használni a mesterséges intelligenciát, hogy becsapjon?

- Egy személy megszemélyesítése hang, kép vagy videó formájában.
- Téged ábrázoló hamis meztelen képek vagy videók (deepfake) készítése zsarolás céljából.
- Olyan illegális és felkavaró tartalmak előállítása, amelyek megtekintése traumatizáló hatású lehet.

Mindezek tudatában fontos, hogy óvatosan kezeld az online megjelenő tartalmakat, és ne higgy el mindent, amit látsz vagy hallasz. Mindig gondolkodj kritikusan, és figyelj azokra a jelekre, amelyek arra utalnak, hogy valami esetleg MI által generált lehet.



MI által generált kép

Hogyan ismerheted fel az MI által generált tartalmakat?

Az MI által generált tartalmak megtévesztőek lehetnek, de egy kis odafigyeléssel jól felismerhetők. Először is, keress olyan dolgokat, amelyek valamiért nem tűnnek valósnak – például túlságosan fényes képeket, túl tökéletesnek tűnő szövegeket, vagy furcsa hibákat, például torz kezeket a fotókon vagy esetlen mondatszerkezeteket a szövegben. A mesterséges intelligencia eszközei képesek olyan tartalmakat létrehozni, amelyek valóságosnak látszanak és hangzanak, de olykor hiányzik belőlük az emberi munkára jellemző természetesség vagy éppen az apró hibák.

A másik ötlet a tényellenőrzés. Az MI által generált tartalom, különösen, ha szövegről van szó, olyan információkat közölhet, amelyek meggyőzően hangzanak, de nem pontosak vagy hitelesek. A fordított képkereső eszközökkel ellenőrizni tudod, hogy egy képet generáltak vagy megváltoztattak-e. Különösen vigyázz a népszerű vagy szenzációhajhász tartalmakkal: ezek gyorsan terjedhetnek, de gyakran félrevezetőek vagy hamisak.

Ha olyan tartalommal találkozol, amelyről tudod, hogy hamis vagy félrevezető, nem elég figyelmen kívül hagynod, mindenképp jelentsd is. A legtöbb platformon van valamilyen funkció a hamis tartalmak megjelölésére vagy bejelentésére, ami segíthet megakadályozni a félretájékoztatás további terjedését.

Biztonságos játék az interneten

A számítógépes játék a készségekről, a kihívásokról és a hasonló érdeklődésűekkel való kapcsolatteremtésről szól. Ahhoz, hogy jól érezd magad, ugyanakkor biztonságban is legyél, elengedhetetlen, hogy tisztelettudó és támogató módon játssz. Ez azt jelenti, hogy kedvesnek kell lenned a játékostársaiddal, tisztességesen kell játszanod, és tiszteletben kell tartanod a többieket. A pozitív hozzáállás és mások elfogadása által mindenki számára javulhat a játékélmény.

Az online megismert játékosok közül azonban nem mindenki fog tisztességesen játszani. Légy résen, figyelj az intő jelekre, és ne bízz meg túl könnyen másokban. Mindig tartsd titokban a személyes adataidat, mint például a teljes nevedet, a lakcímedet vagy az iskolád nevét. Ha valaki a csevegés során kellemetlen helyzetbe hoz, lépj ki, vagy némítsd el a beszélgetést. A biztonságod mindennél fontosabb, ezért habozás nélkül blokkold vagy jelentsd a sértegető, kártékony játékosokat.

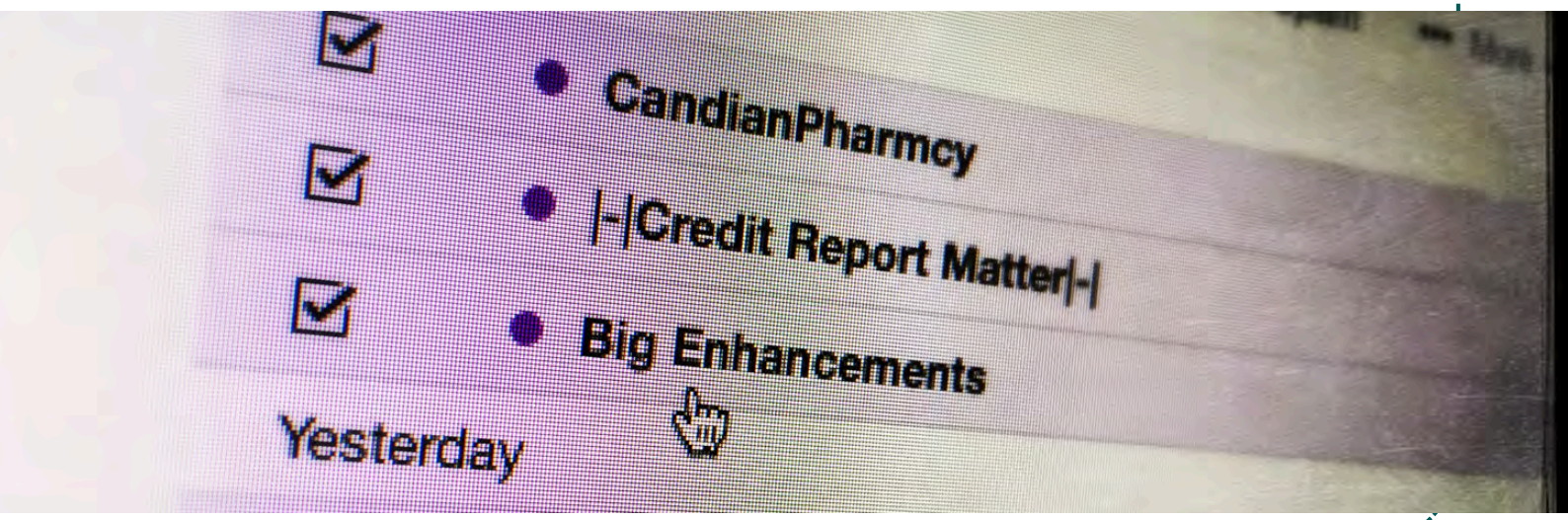
Ne feledd, hogy a játékosközösségekben előfordulhat, hogy egyeseket kirekesztenek, és egyes csoportok tagjai gyakrabban válnak ennek célpontjává. Fontos, hogy vigyázzatok egymásra, és segítsétek egymást, különösen azokat, akik sérülékenyebbek. Ha kirekesztő viselkedést vagy zaklatást tapasztalsz, vagy ilyennek leszel tanúja, emelj szót, és bátran kérj segítséget. Szólj valakinek, akiben megbízol, akár egy barátnak, családtagodnak, de külső segítséget is kérhetsz. Összefogással és a felmerülő problémák kezelésével mindenki számára pozitívabb és befogadóbb játékkörnyezetet lehet teremteni.

Mit jelent az adathalászat?

Az adathalászat egy olyan csalási módszer, amikor a csalók egy megbízható vállalatnak vagy személynek adják ki magukat, hogy ezáltal rávegyenek a személyes adataid vagy például a jelszavad megosztására. Az adathalászok e-maileket, üzeneteket vagy hamis weboldalakat használnak fel erre a célra. Előfordulhat, hogy egy bajba került barátnak adják ki magukat, aki szívességet kér, vagy egy jó hírű cég nevében állítják, hogy nyertél valamilyen díjat.

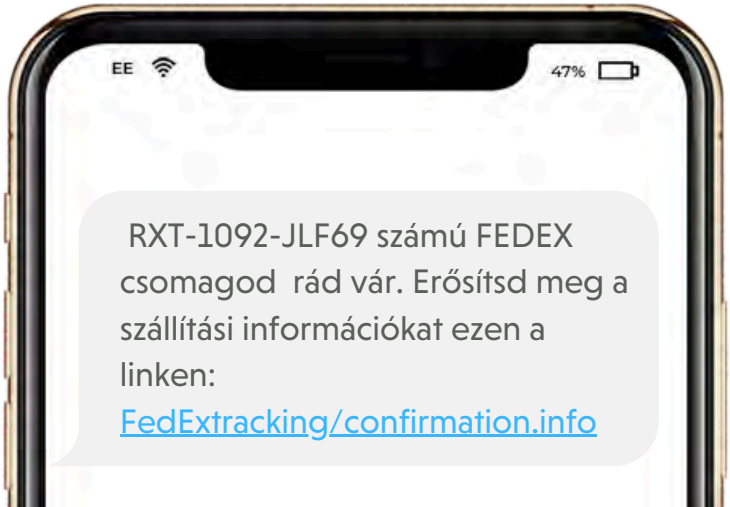
Vigyázz, ha a következőket tapasztalod:

- Sürgetés, amivel a csalók gyakran próbálnak pánikot kelteni, hogy gyors cselekvésre késztessenek.
- Általános üdvözlések, amelyekben nem szerepel a neved.
- Hibásan írt URL-címek vagy apró eltérések a cég nevében.
- Nem várt nyeremények vagy ajándékok, amelyeket egy linken keresztül regisztrálva kaphatsz kézhez.



Ha adathalász linkekre kattintasz, az nem csak a készülékedre jelenthet veszélyt, de emellett még rosszindulatú szoftverekhez, személyazonosság-lopáshoz vagy a fiókjaidhoz való jogosulatlan hozzáféréshez is vezethet. Mielőtt egy linkre kattintasz, gondolj mindig a biztonságodra, és alaposan nézd meg az URL-címet. Ha furcsán néz ki, vagy elírás szerepel benne, semmiképpen ne kattints rá. Mindig ellenőrizd az e-mailek vagy az üzenetek forrását és a weboldalak megbízhatóságát, mielőtt bármilyen lépést tennél.

Különösen gyakori az SMS-ben történő adathalászat, más néven „smishing", amely ismerősöktől vagy cégektől érkező sürgős üzenetek formájában jelenik meg, és amelyben arra kérnek, hogy kattints egy linkre, vagy add meg a személyes adataidat. Mindig legyél óvatos, ha olyan üzenetet kapsz, amelyre nem számítottál. Különösen, ha azt állítják benne, hogy egy segítségre szoruló családtagtól érkezett.



Szexting: Amire vigyázni kell

A szexualitás felfedezésének és az emberekkel való kommunikációnak része lehet az üzenetben történő flörtölés és az intim képek küldése. Sok fiatal és felnőtt kipróbálja a szextinget, és amikor ez beleegyezéssel és minden érintett tiszteletben tartásával történik, akkor pozitív megélés is lehet. Van azonban néhány fontos dolog, amit mindenképpen fontolj meg, mielőtt intim kép küldése mellett döntenél.

BELEEGYEZÉS

Minden érintettnek maximálisan komfortosan kell éreznie magát a képküldéssel kapcsolatban. Ha valamelyikőtök úgy érzi, hogy ez neki nem fér bele, bátran mondjatok nemet, bármikor dönthettek úgy, hogy nem küldtök intim képet.

KOMMUNIKÁCIÓ

Beszéljetek világosan az elvárásaitokról. Egyezzetek meg a határokban, és beszéljétek meg, hogyan gondoskodtok majd az egymásnak küldött képek és üzenetek védelméről.

MEGÉRZÉSEK

Figyelj a szextinggel kapcsolatos megérzéseidre. Ha kétségeid támadnak miatta, bármikor kiszállhatsz, és jogod van nemet mondani.

A szexting csak úgy lehet biztonságos és pozitív élmény, ha minden érintett jól és komfortosan érzi magát a helyzetben. A személyes üzeneteket soha ne oszd meg, és ne mutasd meg senki másnak, és ügyelj arra, hogy a privát tartalmat biztonságosan, mások számára nem hozzáférhető módon tárold.

Szextinggel történő visszaélés

A szexting személyes dolog, de előfordulhat, hogy a dolgok nem a tervek szerint alakulnak, és visszaélnek a képeiddel. Ha valaki a beleegyezésed nélkül megosztja vagy továbbítja a rólad készült intim képeidet, azt szextinggel való visszaélésnek nevezik, ami megtörténhet véletlenül, vagy akár szándékosan is. Ez nem jogszerű, és soha nem a te hibád – a felelősség teljes mértékben azt a személyt terheli, aki az engedélyed nélkül megosztotta a képedet. Ha ez megtörténik veled, teljesen normális, hogy dühösnek, lesújtottnak érzed magad. De sose feledd: nem vagy egyedül, és nem te vagy a hibás!
Világszerte több ingyenes szolgáltatás áll rendelkezésre, amelyek segítenek az ilyen helyzetekben. Érdemes megkeresni valamelyik lelkisegély-szolgáltatást vagy hotline-t, ahol érzelmi támogatást, tanácsokat vagy ötleteket kaphatsz ahhoz, hogy a képeidet a lehető leggyorsabban el tudd távolíttatni az internetről.

Ha valaki azzal fenyeget, hogy megosztja a privát üzeneteidet vagy képeidet, azt szexuális célú zsarolásnak nevezik. Ez esetben a zsaroló személy a képek titokban tartásáért cserébe pénzt vagy még explicitebb tartalmakat kér, esetleg személyes találkozóra akar rákényszeríteni. Ez rettenetesen stresszes és nyomasztó érzés lehet, de ne feledd: soha nem te vagy a hibás. A segítség mindig elérhető, és vannak szakemberek, akik készségesen támogatnak. Források és támogatás kérése itt, itt és itt érhető el.

Mi a helyzet az online térben kötött ismeretségekkel?

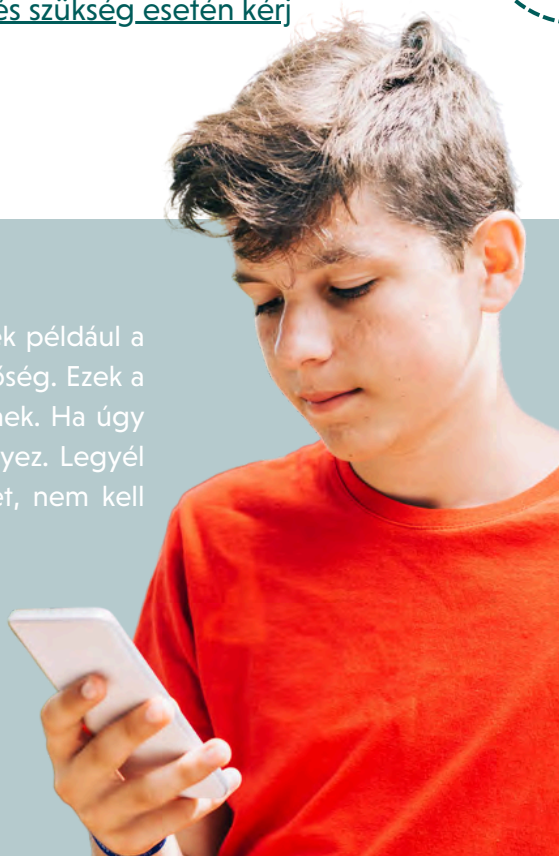
Az online ismerkedés rendívül elterjedt, és az egymás számára idegenek is hamar érezhetik úgy, mintha mindig is ismerték volna egymást. De mi történik akkor, ha az online barátod valójában nem az, akinek kiadja magát? Ha magánjellegű dolgokat kezd kérdezni, vagy szexuális irányba tereli a beszélgetést, akkor lehet, hogy behálózni, becserkészni próbál, amit angolul groomingnak nevezünk.

A behálózók olyan felnőttek, akik az interneten kortársnak adják ki magukat, hogy elnyerjék a bizalmadat, és manipulációval szexuális kapcsolatra vegyenek rá. Mesterei a megtévesztésnek, ami megnehezíti a valódi szándékaik felismerését. Ne feledd, soha nem a te hibád, ha bedőlsz a módszereiknek – a behálózók szándékosan élnek vissza a bizalmaddal, és kihasználják a barátságotokat. Bárkivel előfordulhat, hogy egy behálózó célpontjává válik, ugyanakkor vannak, akik kiszolgáltatottabbak, így például egyes marginalizált csoportok tagjai.

Figyelj az intő jelekre, manipuláció vagy az irányító szándék jele lehet, ha valaki az online kapcsolat titokban tartását kéri tőled. Az egészséges és tiszteletteljes kapcsolatokat nem kell titkolni. Az igazi barátok nem hazudnak, és nem kényszerítenek semmi olyanra, ami számodra kényelmetlen. Ha valakinek a személyazonosságát illetően bizonytalan vagy, kerüld a személyes adatok megosztását, és próbáld ellenőrizni állításai hitelességét. Ha azt tervezed, hogy találkozol egy online térben megismert személlyel, mindig szólj a szüleidnek, és vigyél magaddal egy megbízható barátot.

Mire kell vigyázni az interneten?

Akárcsak a való életben, az interneten is fontos odafigyelni minden olyan jelre, ami nem tűnik helyesnek, vagy rossz érzést kelt benned. Egyesek megpróbálhatnak olyan dolgokra kényszeríteni, amelyek nem tetszenek neked, akár zaklatással, nem kívánt képek küldésével vagy akár érzelmi manipulációval. Ne feledd: ezeknek a viselkedésformáknak mindegyike káros és elfogadhatatlan. Bízz a megérzéseidben – jelentsd be, és szükség esetén kérj támogatást.



JÓ TANÁCS

Figyelj oda a barátaid viselkedésében történt hirtelen változásra, amelyek például a következők lehetnek: visszahúzódás, titkolózás vagy túlzott készülékfüggőség. Ezek a jelek arra utalhatnak, hogy az interneten valamilyen problémával küzdenek. Ha úgy érzed, valami baj lehet, legyél te az a barát, aki beszélgetést kezdeményez. Legyél együttérző, és tudasd vele, hogy nyugodtan elmondhatja a történteket, nem kell félnie az ítélkezéstől.

Kezdheted valami ilyesmivel: „Újabban úgy veszem észre, mintha nem lennél a régi. Ha szeretnél beszélni róla, szívesen meghallgatlak." A támogatásod sokat jelenthet a barátodnak, ezért tudasd vele egyértelműen, hogy bátran elmondhatja, mit tapasztalt, és hogy nem kerül bajba, ha őszinte lesz.

3. SZAKASZ

Segítségkérés

Segítségkérés

A biztonságod és a jólléted mindennél fontosabb. Ha zaklatnak, zsarolnak, vagy ha a privát képeid kerültek ki az internetre, habozás nélkül beszélj valakivel, akiben megbízol – például egy baráttal, családtaggal, tanárral, vagy keresd a lelkisegély-szolgálatokat. Ne felejtsd el, hogy a lelkisegély-szolgálatoknak titoktartási kötelezettségük van, és az a dolguk, hogy ítélkezés nélkül segítsenek a hozzájuk fordulóknak. Soha nem kell egyedül szembenézned ezekkel a nehézségekkel. Mások is átmentek már hasonló küzdelmeken, és számtalan szervezet kifejezetten azért jött létre, hogy támogatást nyújtson ilyen esetekben. Ha nehéz vagy veszélyes helyzetbe kerültél, tudnod kell, hogy mindig van segítség.

Segélyvonalak megkeresése

Az online fenyegetések hatására túlterheltnek, zavarodottnak vagy ijedtnek érezheted magad – és ez teljesen normális. A segélyvonalak olyan biztonságos és bizalmas teret biztosítanak, ahol nyíltan beszélhetsz az aggályaidról, és segítséget kaphatsz a helyzeted megoldásához. A segélyvonalakat ingyenesen hívhatod, de SMS-ben vagy chatben is elérheted. A helyi segélyvonal elérhetőségét itt találod.

Jelentsd be a sértő, bántó felhasználókat a platformokon

A közösségi médiának olyan biztonságos térnek kellene lennie, ahol beszélgethetsz a barátaiddal, kifejezheted magad, és kreatív lehetsz. Ha valamilyen furcsa dologgal szembesülsz, jelentsd be – akár nem megfelelő tartalomról, akár valakinek az ártalmas, bántó viselkedéséről van szó. A legtöbb közösségimédia- és videójáték-platformon van bejelentés funkció. Keresd meg a beállítások vagy az opciók menüpontban, és élj ezzel a lehetőséggel.

Jelentsd be az ártalmas online tartalmat a helyi hotline-nál

A hotline-ok azon dolgoznak, hogy gyorsan eltávolítsák az online szexuális visszaélésekkel kapcsolatos tartalmakat az internetről. Ha kiszivárgott valamilyen rád vonatkozó intim tartalom, vagy ha bármikor gyermekeket érintő intim tartalommal találkozol, jelentsd be. Az összes kontinensre kiterjedő, hotline-okból álló hálózatunk és elemzőink kifejezetten fel vannak készítve az ilyen helyzetek kezelésére. A helyi hotline elérhetőségét itt találod.

Take It Down

A Take It Down-szolgáltatás: Ha elmúltál már 18 éves, de egy olyan intim kép került ki rólad az internetre, amely még 18 éves korod előtt készült, a Take it Down segítségedre lehet azzal, hogy a tartalmat eltávolítja az internetről.

Szeretnél többet tudni az internet biztonságos használatáról? Akkor keresd fel a helyi lehetőségeket, melyekről itt vagy itt tájékozódhatsz. Ezek a platformok biztonsági tippeket, forrásokat, útmutatást és tanácsokat kínálnak a biztonságosabb online élmények érdekében.

Hivatkozások

- Cyberbullying – Mást bántani nem menő
- Internet Hotline beszámoló 2023
- Kézikönyv gamer gyerekekhez
- Jól van a gyerek, ha játszik? – Tudástár videójátékokról szülőknek és pedagógusoknak
- Van eszköz a kezedben (Útmutató a digitális szülői felügyelet alkalmazásához)
- Szűrőszoftver-katalógus
- Sztorik a zsebben – Történetek a közösségi médiából
- Mit lájkol a gyerek? Szülőknek a közösségi médiáról
- Gyermekeink online biztonsága a megfelelő eszközbeállításokkal kezdődik
- Vigyázó szemetek az adataitokra vessétek! – az adatvédelemről egyszerűen
- Phishing – mindent az adathalászatról és annak kivédéséről
- Túl szép, hogy igaz legyen: a csaló webshopok veszélyei és felismerése
- Szexting – így beszélj a gyerekeddel a témáról!
- Bűvösvölgy Médiaértés-oktató Központ weboldala
- Bűvösvölgy Tudástár – óravázlatok tanároknak
- Gyerek a neten weboldal szótárral, kvízzel, részletesebb írásokkal

„Az Európai Unió finanszírozásával. Az itt szereplő vélemények és állítások a szerző(k) álláspontját tükrözik, és nem feltétlenül egyeznek meg az Európai Unió vagy az Európai Oktatási és Kulturális Végrehajtó Ügynökség hivatalos álláspontjával. Sem az Európai Unió, sem az Európai Oktatási és Kulturális Végrehajtó Ügynökség nem vonható felelősségre miattuk."

INHOPE

Együtt erősebbek vagyunk - Útmutató a digitális műveltséghez fiataloknak, szülőknek, gondviselőknek, tanároknak és hotline-oknak.

További információ: inhope.org

Az Európai Unió támogatásával