**INTERNETBIZTONSÁG**

*Bemutatkozás (Név, munkakör, esetleg, hogy miért vállalkoztam erre a beszélgetésre)*

*Az alábbi Kahoot játékkal tesztelhető a gyerekek tudása a témában, ha az idő engedi, érdemes az előadást ezzel kezdeni. Amennyiben nincs mindenkinél okostelefon a csoportos játék funkció használatával többen is használhatnak egy eszközt!*

*A tesztet itt tudjátok elindítani*

<https://play.kahoot.it/#/?quizId=dbc4357b-d0cc-4298-8879-b040c38d4a72>



*A játékosoknak pedig az alábbi felületen kell a megadott azonosítóval bejelentkezni a játékba:*

<https://kahoot.it/>

**Bevezető**

Amikor megszületett az internet, mindannyian egy millió szállal egymáshoz kötődő globális közösség részévé váltunk – ez pedig ablakot nyitott számunkra az egész világra. Végérvényesen megváltozott az életünk. A digitális világ - generációktól függetlenül - mindannyiunkat újfajta kihívások elé állít, minket felnőtteket éppúgy, mint titeket. Ezért nem tanácsokat osztogatni jöttünk, hanem hogy beszélgessünk arról, hogyan lehet biztonságban jelen lenni a világhálón, milyen lehetőségeink vannak, hogy kellőképpen felkészüljünk a digitális világ kihívásaira.

Ma világszerte 7 milliárd ember 12 milliárd „okos” eszközt csatlakoztat az internetre- és ez az adat mire kimondtam, valószínűleg máris elavult! Gondolnátok-e, hogy Magyarországon kevesebb mint 10 millióan 12 millió SIM kártyát használunk, vagyis fejenként 1 nél több okoseszköz jut mindenkire, a dédit és a kishugit is beleszámítva.

*Otthon, a családban nálatok hány okoseszköz van?*

*(Minden kérdésnél hagyjuk kicsit beszélni őket – az aktivitászuk eleinte akadozhat, de az idő rövidsége miatt azt se engedjük, hogy túl sokat kommenteljenek!)*

Az elmúlt időben a webre kötött gépek, az okos eszközök számának ugrásszerű megnövekedésével újabb fogalmak jelentek meg, mint az IOT (internet of things)

*Milyen példákat tudnátok felsorolni IOT eszközökre?*

Létezik már okosporszívó; okosvilágítás, ahol telefonjainkról állíthatjuk az izzók fényének színét, irányíthatunk fűtést vagy klímát, de biztonsági szakértők fedeztek már fel okoshűtőkből álló zombihálózatot is. *(Ez a hálózat spam üzeneteket küldött szerteszét a világba.)* Ti is láthatjátok, hogy ez mekkora kontrasztot jelent ahhoz képest, mikor 1991-ben megjelent az első webkamera: ekkor a feltalálók csupán egy kávéskanna tartalmát szerették volna látni távolról, hogy érdemes-e elindulni kávézni. *(A cambridge-i egyetemen történt, diákok fejlesztették és tesztelték, percenként 1 képkockát továbbított a kamera.)*

*Milyen pozitív változást hozott az internet megjelenése, mire használjátok, ahol megkönnyíti az életeteket?*

*Jó esetben az alábbiak mindegyike elhangzik, ha nem egészítsük ki az általuk elmondottakat: tanulás (keresők használata) szocializáció, kapcsolattartás ( e-mail, Skype, messenger, Viber)információszerzés, felfedezés, szórakozás, bevásárlás, ügyintézés*

Látjuk az internet előnyeit, most vegyük sorra az árnyoldalakat

*Mit gondoltok, milyen potenciális kockázatok jelentek meg az internethasználat elterjedésével?*

*Pld: a következőket emeljük ki, amennyiben nem sorolják fel: A munka elvesztése a rossz online hírnévnek köszönhetően; online zaklatás; pénzügyi veszteség (online vásárláskor bankkártya adatok ellopásával ); személyes adatokhoz való hozzáférés; Spyware, adware vagy más nyomkövető szoftver feltelepülése a készülékekre stb.*

Vegyük sorba, mik azok a számunkra legértékesebb dolgok, amiknek a védelméről feltétlenül gondoskodni kell! Az első ilyen a:

1. **SZEMÉLYES MÁRKA**

(*A téma boncolgatására egy külön órát szánunk, így csak dióhéjban említsük meg a lényeget*)

Minden, amit online közzéteszel, akár egy egyszerű fotó is, a hírneved részévé válik az életed hátralévő részében. Szóval, mielőtt posztolnál, kérdezd meg magadtól:

• Bánthat ez másokat?

• Megosztanám ugyanezt a szüleimmel?

• Milyen hatással lesz ez a jóhíremre, okozhat-e a későbbiekben kínos pillanatokat? (még egy 20 éves kép is bármikor előkerülhet egy állásinterjún – ne kelljen szégyenkezned miatta)

Gondoltátok volna, hogy 2013-ban összesen 16300 évnyi időt töltöttünk el azzal, hogy az online reputációnkon esett csorbát megpróbáljuk kiköszörülni!

1. [**TÁRSAS**](https://www.microsoft.com/en-us/digital-skills/online-safety?activetab=protect-whats-important%3aprimaryr4) **KAPCSOLATOK (család, ismerősök, barátok)**

A kapcsolatok fenntartása, kezelése a való életben és az online térben sem egyszerű.

Például, ha konfliktusba keveredsz a testvéreddel lerendezhetitek egy párnacsatával, de akár szócsatát is vívhattok a messengeren keresztül.

*Soroljatok fel olyan helyzeteket, amikor a személyes kommunikáció az előnyösebb, és olyanokat, amikor érdemesebb online tartani a kapcsolatot!*

Például az online kapcsolattartás könnyebb olyasvalakivel, aki hosszú távon, nagy távolságra van tőlünk, mondjuk külföldön

Személyes eszmecsere szerencsésebb, ha pld nem vagyunk biztosak a másik fél szándéka felől - ilyen esetben a testbeszéd a szemkontaktus sokat segíthet.

**Ismerkedés a neten**

*Előfordult már, hogy olyasvalakivel beszélgettél online, akit nem ismersz személyesen? Hogy kerültél vele kapcsolatba? Ha igen, mit akartak tőled? Mit csináltál? Hogyan reagáltál?*

*(figyeljünk az időre, ne engedjük szabadjára a sztorizgatást!)*

*Levetíthetjük az alábbi linken látható „Predators” videót.*

<https://www.youtube.com/watch?v=j-WvhDziQtU>

Az emberek nem mindig azok, amiknek mondják magukat. Sokan úgy tesznek, mintha gyerekek vagy tizenévesek lennének, hogy gyanútlanul szóba álljatok velük a neten. Használhatnak hamis profilképet, és ezen túlmenően is olyan profiladatokat adhatnak meg, hogy ártalmatlannak, megbízhatónak tűnjenek. Ez nem jelenti azt, hogy mindenkire gyanakodnod kell, de óvatosnak kell lenned az online ismerősökkel kapcsolatban. Mire figyelj:

* Facebookon csak azt igazold vissza, akivel ténylegesen ismeritek egymást!
* Az ismerőseid listáját ne add ki a kezedből, állítsd be, hogy ne, vagy csak korlátozottan legyen látható!
* Ha valaki hízelgő online, akkor óvatosnak kell lenned. Bár sok ember valóban kedves, a ragadozók használhatják a hízelgést, mint eszközt, hogy megpróbáljanak kapcsolatba lépni veled.
* Ne beszélgess olyasvalakivel, aki, aki túlságosan személyes kérdéseket tesz fel. Egyszerűen szakítsd meg a vele való beszélgetést!
* Ha kényelmetlenül érzed magad egy online beszélgetés során, szólj a szüleidnek vagy más megbízható felnőttnek.
* Mentsd el az e-maileket vagy egyéb kommunikációt is, mert ezek szükség esetén bizonyítékként szolgálhatnak a nem megfelelő viselkedésre
* Soha ne találkozz személyesen felnőtt kíséret nélkül olyannal, akivel eddig csak online álltál kapcsolatban! Ha valaki nagyon szimpatikus és szívesen barátkoznál vele személyesen is, erre is van lehetőséged, de ebben az esetben feltétlenül kérd a szüleidet, vagy más megbízható felnőttet, hogy kísérjenek el a találkozóra!
1. **ADATVÉDELEM- személyes adatok védelme**

Ha adatvédelemről beszélünk, sok mindenre oda kell figyelni, hiszen több oldalról is megközelíthetők a személyes adataink. Már ha hagyjuk - hiszen sok esetben mi magunk is tehetünk azért, hogy adataink a lehető legkevésbé legyenek hozzáférhetők. Célszerű digitális személyiségünket annyiféle módon kell védeni, amennyire csak lehetőségünk van!

Mint mindig, a legfontosabb a megelőzés, azaz figyeljetek oda, milyen adatokat közöltök magatokról és ki láthatja ezeket, legyen szó közösségi oldalakon lévő profilról, képekről, levelezésről, vagy applikációk használatáról.

*Melyek a legérzékenyebb személyes adatok, amiket semmilyen körülmények között vagy csak nagy körültekintéssel szabad megosztani a világhálón? (életkor, születési dátum, lakcím, iskola, telefonszám)*

*Feltennél-e olyan fotót a netre, ahol – akárcsak a háttérben is – látható a személyi- vagy a diákigazolványod száma, útleveled? Milyen veszélyt rejtenek ezek a képek, hogyan lehet visszaélni velük?*

A közvetett információk is árulkodhatnak, pld közzétett iratokból adódhat személyazonosság lopás vagy pld családi nyaralásról real -time közölt képek esetében megtudható, hogy épp senki sem tartózkodik a házban.

Mit tehetsz, hogy elkerüld, hogy a személyes adataid illetéktelen kezekbe kerüljenek?

* Mielőtt lenyomod az entert-t, kérdezd meg magadtól megosztanád-e ezeket az információkat magadról egy ismeretlennel?
* Egy nyomozó alaposságával nézz át minden képet, amit posztolni kívánsz, megvizsgálva a hátteret is, tartalmaz-e személyes információkat.
* Egyes webhelyek megkövetelik, hogy részletes profilt töltsünk fel. Légy résen, ha a használni kívánt webhelyek és alkalmazások teljes nevet, születési dátumot, címet, telefonszámot vagy más személyes adatot kérnek. Mielőtt átadnád ezeket a részleteket, gondold át, hogy vajon miért van szükségük ezekre az adatokra, hiszen az összes átadott információnál fennáll, hogy rossz kezekbe kerül, vagy akár egy harmadik félnek (akár csalóknak) eladhatóvá válik.
* Számos webhely lehetővé teszi, hogy korlátozd, ki láthatja a profilodat, - minden felhasználói fióknál módosítsd a beállításokat az adataid védelmének érdekében.
* Ne feledd, hogy a közösségi médiacsoportok, amelyekhez csatlakozol (például szakkör, vagy sportszakosztály) nyilvánosak lehetnek, és a csoportbeállítások vonatkoznak rád is!

**A privát profil a jó profil! Te döntöd el, mennyi információt adsz ki magadról!**

1. **Milyen a jó jelszó?**

„A jelszó olyan, mint a fehérnemű:

* cseréld rendszeresen,
* ne hagyd szem előtt,
* ne add át másnak!”
* Használj erős jelszót a kutyád neve, vagy a születési dátumod helyett!

Ha valaki megszerzi a felhasználónevünket, ami viszonylag könnyen hozzáférhető, a leggyakoribb jelszavak próbálgatásával bejuthat a fiókunkba. Használj erős jelszavakat, amelyek legalább nyolc karakter hosszúak, beleértve kis és nagy betűket, a számokat és a speciális szimbólumokat, és ne tartalmazzon személyes adatokat. (Nevek, születésnapok, cím és egyszerű sorozatok, mint 12345). A csalók ezekkel próbálkoznak először!

* Minden accounthoz érdemes más és más jelszót használni, így elkerülhető, hogy ha valaki az elővigyázatosság mellett mégis áttöri a védelmet, az összes fiókotokhoz egyetlen jelszóval hozzáférjen.
* A jelszavakat időnként cseréljétek le; erre sok oldal külön felszólítást is küld. A könnyebb megjegyezhetőség kedvéért alakítsatok ki saját szisztémát a jelszavak változtatására.
* Ha nyilvános számítógépen, például az iskolában vagy a könyvtárban internetezel, győződj meg róla, hogy az automatikus bejelentkezési funkció le van tiltva, és mindig jelentkezz ki a fiókjaidból, mielőtt elhagyod a gépet. A böngésző bezárása nem elég!
* A jelszavaidat tartsd titokban, még a barátaidnak se add meg!
1. **Phishing**

Az erős jelszavak, egy jól beállított tűzfal és egy rendszeresen frissített adatbázissal rendelkező vírusirtó megfelelő védelmet nyújthat a betolakodókkal szemben, ám a csalók sokkal trükkösebb módszereket is bevethetnek az adataitok megszerzésére, ezeket Phising-nek, vagyis adathalászatnak, adatbányászatnak hívjuk.

A csalók jellemzően kéretlen email formájában keresik meg az óvatlan áldozatokat, de előfordul, hogy telefonon hívnak adategyeztetés miatt olyan cég nevében, amellyel kapcsolatban állsz. Bankok, iskola, rendszergazdák és komolyabb cégek sosem kérik be a jelszavadat és felhasználónevedet, főleg nem e-mailben, ezért ne válaszolj még akkor sem, ha a levél hivatalosnak vagy fenyegetőnek tűnik!

Ne nyiss meg, és ne olvass el ismeretlen feladótól érkező levelet! A levél vagy a csatolmánya vírusokat telepíthet a számítógépre, pld legutóbb a futótűzként terjedő ún. zsarolóvírust.

Sajnos nem csak ismeretlenektől, hanem barátainktól érkező csatolmány vagy hivatkozás is tartalmazhat vírusokat és kémprogramokat, amennyiben a csalók hozzáférést szereztek az ő fiókjaikhoz, ezért óvakodjunk a „fura” levelek és csatolmányok megnyitásától ( pld ha a barátod a leckét szeretné megosztani veled e-mailben, ezt előzőleg valószínűleg más csatornákon – pld cseten, telefonon - előre egyeztetitek)

* Ne dőlj be az olyan hívásoknak, e-maileknek sem, amiben arról értesítenek, hogy nyertél, de csak akkor kapod meg, ha elküldöd az adataidat.
* Ha ismeretlen (külföldi) telefonszámról hívnak – céljuk, hogy visszahívd a számot. Ne tedd! pld. Feltöltetik veled a saját kártyás egyenlegüket. Gondold végig, miről akarna veled bárki ismeretlen külföldről beszélni?
* Ha számlát kapsz elektronikusan, ne fizess egyből (pl. Telekomos átverés a számlatartozásról)
* Mielőtt bármit vásárolnál az interneten, győződj meg róla, hogy az URL https-el kezdődik (az 's” secure, azaz biztonságos), ellenkező esetben a hackerek ellophatják a bankkártya adataidat. Egyes webhelyek nem használnak titkosítási szoftvert, így védtelenné válnak a hackertámadásokkal szemben. A bal felső sarokban egy zárt lakat icon is jelöli, ha a webhely biztonságos.
* Bármikor kérheted az adataid és mail címed törlését az egyes alkalmazások adminjaitól és leiratkozhatsz a kéretlen hírlevelekről!
1. **MOBIL ESZKÖZ BIZTONSÁGA**

*Számítógépen vagy mobilon interneteztek szívesebben, és miért pont azon?*

**a. Védd a mobilodat!**

 Az utóbbi évek felméréseiből az derül ki, hogy a nethasználat a számítógépekről egyre inkább a mobiltelefonok irányába tolódik, különösen az ifjabb, „z” generáció számára, amihez ti is tartoztok. Ennek számos előnye van; pld tartalmasan tölthetitek az utazási időt (tanulás, podcast vagy zenehallgatás, chat a barátokkal), viszont mindenképpen célszerű mobileszközeinket is ellátni a megfelelő PIN kóddal és egyéb védelmi megoldásokkal, legyen az ujjlenyomat-leolvasás vagy hagyományosabb, számkódos képernyőzár és jelszavas védelem.

* állíts be képernyőzárat! – ha csak néhány percre, de illetéktelen kezekbe kerül a mobilod, nagy bajt okozhat ( üzeneteket küldhetnek róla, képeket tehetnek közzé stb)
* Mobiltelefonon is kaphatsz vírusokat! Töltsd le a gyártótól származó biztonsági frissítéseket és légy óvatos az egyéb programok vagy alkalmazások letöltésekor.
* Kerüld az ingyenes ajánlatokat és ingyenes csengőhangokat, ezek gyakran tartalmaznak rosszindulatú programokat.
* A nyomonkövetés funkció beállításával akár az örökre elveszettnek hitt eszközök is előkerülhetnek!
* Csak akkor vedd elő a mobilodat, ha nyugalomban vagy, és nem kell másra koncentrálnod! (pld metrón ülve) Ha gyalogosan közlekedsz még a zenehallgatás is életveszélyes lehet, hiszen minden érzékszervünkre szükség van a veszélyek elkerüléséhez, így a hallás legalább olyan fontos, mint a látás! Később, amikor jogosítványt szereztek ennek még nagyobb jelentősége lesz, hiszen vezetés közben tilos a mobilhasználat, mivel egy másodpercnyi figyelmetlenség, is súlyos balesetet okozhat. Minden üzenet, SMS várhat addig, míg a kocsi megáll!

**b. Külső adathordozók**

Soha ne csatlakoztass a készülékedhez ismeretlen forrásból származó adathordozót - vírusokat rosszindulatú szoftwereket tartalmazhatnak! Ha gazdátlan pendrive-ot vagy CD -t találsz, győzd le a kíváncsiságodat, és ne kockáztasd az eszközeidet.

*Itt levetíthetjük a következő videót*

<https://www.youtube.com/watch?v=3pNAQH0BDJg>

1. **Geolocation**

Számos mobilalkalmazás egy olyan funkciót használ, amely kéri, hogy osszuk meg tartózkodási helyünket másokkal. Jó ötletnek tűnhet, mikor a Facebookon a barátaitok irigykedve értesülhetnek arról, hogy épp milyen remek helyen vagytok, de rosszindulatú egyének éppoly könnyen felhasználhatják ezt az információt és megtudhatják, hol érhetnek utol benneteket.

Bizonyos alkalmazások (például térképek és útvonaltervek alkalmazásai) helyalapú szolgáltatásokat igényelnek, de nem teszik közzé a tartózkodási helyet, vagyis illetéktelenek nem férnek hozzá ehhez az információhoz.

1. **Nyilvános wifi - Wi-Fi hotspotok**

Mobileszközzel gyakran csatlakozhattok nyilvános wifi hálózatokhoz éttermekben, üzletekben, parkokban és más helyeken. A hotspotok használata egyrészt remek dolog, hiszen ingyen netezhettek, viszont ne feledjétek, hogy ez kevésbé biztonságos, mint az otthoni internetkapcsolat.

Ha nyilvános wifi hálózatra csatlakozol:

* Védd az eszközödet a tűzfal bekapcsolásával és legyen naprakész a víruskeresőd!
* Tiltsd le az automatikus csatlakozás funkciót. Állítsd be manuálisan, melyik hálózatra kívánsz csatlakozni, pld adott étterem, színház stb wifijére, így elkerülheted a szélhámosok által felállított Wifi csapdákat, amiket adathalászat céljából állítanak fel.
* A Hálózati vagy megosztási beállítások menüben tiltsd le a Fájl- és nyomtatómegosztás funkciót, így illetéktelenek nem férhetnek a tárolt fájlokhoz.
* Nyilvános helyen tartsd szemmel, ki tartózkodik a közeledben, hiszen a vállad fölött átnézve bárki megtekintheti a személyes adataidat és tevékenységedet.
* Soha ne hagyd felügyelet nélkül a tabletedet vagy a mobilkészülékedet! Gondold át mekkora veszteség érhet, és inkább vidd magaddal az eszközeidet a kár a mosdóba is!
* Ne végezz pénzügyi tranzakciót nyilvános wifin, például banki tevékenységet vagy vásárlást, semmit, ahol bankkártya adatokat kell megadni! A bűnözők telepítik a billentyűleütés-felismerő szoftvert a nyilvános számítógépekre, így kémkednek, hogy beléphessenek a fiókodba.

**Adataid biztonságának érdekében általános szabály, hogy légy résen és ha valami gyanúsnak tűnik, bízz az ösztöneidben!**

Leselkednek ránk olyan veszélyek is, amelyek ellen kevésbé tudunk védekezni. Ilyen például a **tracking cookie**, azaz a nyomkövető süti. Netezési szokásaink annyira árulkodók, hogy másoknak értékes információval szolgálhatnak és egész iparágak élnek ezekből. Az interneten rengeteg cég megannyi algoritmusa dolgozza fel a rólunk információkat. Ezek alapján tálalnak személyre szabott hirdetéseket számotokra, így ha kellemetlen tartalom, hirdetés jelenik meg böngészés közben, erről ti magatok is tehettek! Ezt azzal tudjátok befolyásolni, hogy milyen oldalakat böngésztek, milyen hirdetésekre kattintgattok.

Ti is biztosan tapasztaltátok, hogy mennyire testre szabottak például a Google vagy egyéb hirdetési szolgáltató reklámjai böngészés közben. Ez nyomkövetéssel lehetséges, amit viszont egyre több böngészőben van lehetőségünk ezt letiltani - éljünk vele!

**6. BIG DATA**

*Tudjátok-e, mit takar a BIG Data kifejezés*?

Digitális világunkban hatalmas mennyiségű, sokféle adat gyűjtése és automatikus kiértékelése zajlik. A legtöbb internethasználó számára szinte lehetetlen felfogni a keletkező adatok mennyiségét, illetve a feldolgozási módszerek sokaságát. Az adatok olyan mennyiségben zúdulnak ránk, hogy ez a hatalmas mennyiség már saját nevet is kapott: „Big Data”.

Az adatgyűjtés számos helyről származhat, pl. alkalmazások, online játékboltok, mobilszolgáltatók ügyfeleinek tartózkodási hely adatai, viselhető mobil fitness eszközök, közösségi hálózatok, streaming szolgáltatások, közcélú adatbázisok, szupermarketek hűségkártya rendszere, bevásárlások, mobil érzékelők, online kiskereskedelmi rendszerek, vagy hálózatba kapcsolt háztartási eszközök.
Vagyis a digitális tér összes felhasználójának szinte minden tevékenységéhez adatgyűjtés kapcsolódik. Mivel az adatok a nap 24 órájában, szünet nélkül képződnek, szempillantás alatt hatalmas adatmennyiség keletkezik.

Mi történik az adatokkal?

Az összegyűjtött adatokból újabb adatokat generálnak, ami felhasználható például az emberek véleményének tanulmányozására és befolyásolására, egészségügyi kutatásra, vagy vásárlási szokások előrejelzésére. A Big Data elemzés eredményei meglehetősen értékesek a gyártó és szolgáltató vállalatok, bankok, biztosítótársaságok, munkáltatók, tudósok, sőt, még a nyomozó hatóságok számára is. Az adatokat, ugyanúgy, mint bármely más árucikket, a cégek megvásárolják. Ezen a ponton túl a felhasználó nem tudja befolyásolni, hogy ki, és milyen célból kapja meg az adatait, és azokat mire használja.

**7. DIGITÁLIS LÁBNYOM**

Akarva- akaratlanul, jól beazonosítható nyomot hagyunk magunk után az online térben- ezt nevezzük digitális lábnyomnak. Személyes márkánknak digitális lenyomatai keletkeznek, ezek pedig már könnyedén elemezhetők, akár programok segítségével is; következtetni lehet tevékenységeinkre, viselkedésünkre. Ezt szem előtt tartva jó, ha nem osztjátok meg nyilvánosan például az esti futás útvonalát, idejét. Ha mégis meg akarjátok osztani másokkal, akkor úgy állítsátok be, hogy csak azok érhessék el, akik a megfelelő bizalmi körbe tartoznak. Ez nem ördögtől való, a digitális világ velejárója!!!

**Alapigazság: Ha valami kikerül az internetre, hihetetlenül nehéz onnan eltüntetni.**

A virtuális tér is valóság: ami online zajlik, az ugyan-olyan felelősséggel jár, és ugyanúgy lehetnek következményei, mintha a fizikai térben történt volna. Ráadásul az internet nem felejt: amit egyszer feltöltöttek, az fent van akkor is, ha törlik. Bár úgy tűnhet, hogy az online bejegyzések törölhetők, mert a továbbiakban már nem látjuk őket, a közzétett információ valójában már rögzült a világhálón. Ha a pillanat hevében kirohanunk valami ellen, vagy meggondolatlanul bejegyzést teszünk közzé magunkról, amint épp valami nevetséges dolgot csinálunk, a „visszavonás” vagy a „törlés” gomb használata valójában már nem sokat ér. A közzétett kép és szöveg felhasználható büntetőjogi bizonyítékként, kárt okozhat másoknak vagy akár saját magunknak is, hiszen a megosztott tartalom másodperceken belül elterjedhet, és nem követhető, hogy kik és hányan láthatták.

**Ellenőrizd a digitális lábnyomodat!**

1. Keress rá magadra

Írd be a keresőbe a vezeték és a keresztnevedet, és nézd át a találatokat! Ha olyasvalamit találsz önmagadról, ami nem kedvedre való (pld egy számodra kínos fotó, amit mások tettek közzé rólad), kérd meg az ismerősödet, távolítsa el az oldalról. Ha nem ismered a közzétevőt, lépj kapcsolatba az oldal adminisztrátorával és távolíttasd el a nem kívánt tartalmat.

1. Ellenőrizd az adatvédelmi beállításokat

A kedvenc oldalaid adatvédelmi beállításai időnként megváltozhatnak, ezért rendszeresen ellenőrizd, kik láthatják a fotóidat, posztjaidat!

1. Szoftverfrissítés

A számítógépes vírusok és kémprogramok gyakran észrevehetetlen pusztítást végeznek a számítógépen. Ellenőrizd időnként, hogy a programok legfrissebb verziót használod-e, nem hagytad-e figyelmen kívül a frissítésekre vonatkozó felhívásokat, vagy beállíthatsz automatikus szoftwerfrissítést is.

1. Gondolkozz, mielőtt posztolsz

A digitális lábnyom több, mint a keresőben rólunk kidobott találatok; ide tartozik az is amit a közzétett posztok, kommentek és képek alapján mások gondolnak rólad.

Mielőtt bármit közzéteszel az interneten, gondold át, akarod-e, hogy mások ez alapján ítéljenek meg. Az online jelenlétet használd arra, hogy elismerést, megbecsülést szerezz magadnak és a viselkedéseddel eredményeiddel másokat inspirálj!

1. Vizsgáld felül rendszeresen a mobilodat!

Szánj időt arra, hogy megértsd a mobileszközök beállításait, a letöltött alkalmazásokat és azok megosztásának szabályait. Töröld azokat, amiket nem használsz és csak a helyet foglalják.

Semmit ne adj írásba, semmit ne küldj el, amit nem szeretnél, hogy akár az egész iskola lásson! Ne továbbíts olyat, ami visszaüthet! A legjobb barátoddal is iszonyúan összeveszhetsz, a szerelmeddel is szakíthatsz, a düh pedig rossz tanácsadó! A bizalom jó dolog, de könnyen vissza lehet vele élni – ne szolgáltasd ki magad senkinek!

**8. HITELESSÉG, OBJEKTIVITÁS**

Ahogyan növekszik eszközeink száma, úgy tódul elénk egyre több és több információ is, sok esetben különböző forrásból, különböző tartalommal. Ha megkérdőjelezhető vagy egymásnak ellentmondó információkat találtok, mindig tegyétek fel a kérdést: Miért? Vizsgáljátok meg, milyen érdeke fűződik az írónak az írás publikálásához. Az igazság gyakran a több különböző álláspont között bújik meg, **ezért ellenőrizd több forrásból az információt–** mérlegelj, szűrd le a lényeget, vesd össze a leírtakat egymással.

Azért fontos, hogy ezzel a szemlélettel nézelődjetek a weben, mert ahogy ti kutatjátok az igazságot, úgy fognak titeket is megítélni. Ha kíváncsi lesz valaki rátok, a lehető legtöbb forrásból próbál utánatok érdeklődni. Fontos, hogy különböző forrásokból ne adjunk egymásnak ellentmondó információkat. A valósággal szöges ellentétben álló képet se fessünk magunkról, hogy ne tűnjünk hiteltelennek és „skizofrénnek” sem.

Azt mindig is tudtuk, hogy „nem mind igaz, ami a neten van”, de arról csak az utóbbi időben lehet egyre többet olvasni, hogy az álhírek terjesztése (és azon keresztül az olvasók, internethasználók befolyásolása, manipulálása) komplett iparággá nőtte ki magát.

Te is felelős vagy azért, amit megosztasz a neten, akkor is , ha nem te írtad! Ha nem vagy meggyőzve egy hír valódiságáról, inkább ne továbbítsd, így nem járulsz hozzá áloldalak és kamuhírek terjedéséhez.

*Szerintetek hogyan lehet eldönteni, hogy mi a kamu és mi az igaz?*

* Ha valami hihetetlennek tűnik, akkor az általában az is.
* Ha valamit lájkolnod kell ahhoz, hogy megnézhesd, az nem jelent jót.
* Ha nincs feltüntetve a cikk szerzője, az gyanús, még akkor is, ha a legnagyobb hírportálokról van szó.
* Ha korábban még sosem látott, ismeretlen oldalon jelenik meg egy adott tartalom,

keress rá a Google-ban. Ha az oldal nevére kevés a találat, vagy csak az oldalra visszamutató linkek jelennek meg, ne bízz benne!

1. **CYBERBULLYING**

*Előfordult már, hogy pletykák kezdtek terjedni rólad az iskolában egy online bejegyzés vagy hozzászólás miatt? Kiderült, hogy kitől eredt a pletyka?*

*Mit csináltál, amikor megtudtad; sikerült leállítani?*

Az angolul cyberbullyingnek nevezett jelenség sajnos aktuális probléma. A magyar 10-18 évesek 88%-a rendelkezik profillal valamelyik közösségi oldalon, 50%-uk már találkozott olyan tartalmakkal, amelyeket nem értett, 20%-uk úgy érzi, hogy áldozata volt valamilyen zaklatásnak, 10%-uk pedig bevallotta, maga is bántalmazott már másokat a neten.

*„Szerintetek miért lehet veszélyesebb az online zaklatás, mint az, ami a való világban történik?”* *(Hagyj időt a gyerekeknek válaszolni körülbelül 40 másodpercet; egy-egy kulcsszó hasznos lehet, de a hosszas történetmesélést érdemes leállítani.)*

A zaklatás (bullying), mint jelenség nem új keletű, hiszen történhet otthon, az iskolában vagy más közösségekben is, de az internethasználat terjedésével az online zaklatás is megjelent a mindennapokban. A számítógépes zaklatás a fizikainál bizonyos szempontból rosszabb is lehet, hiszen a virtuális felületeken a zaklatótól nem lehet elmenekülni, a bántalmazás nem szűnik meg hétvégén vagy az iskolai szünetben.

Az elektronikus megszégyenítés eszköztára sajnos kimeríthetetlen. A legtöbb áldozat arról számolt be, hogy üzenetekkel zaklatták, a nevében kommenteltek, posztoltak tartalmakat, vagy olyan képeket, videókat tettek közzé, amelyek számára kellemetlenek, kínosak.

*Ezen a ponton levetíthető az alábbi Cyberbullying videó:* [*https://www.youtube.com/watch?v=\_sbo4W9ze3s*](https://www.youtube.com/watch?v=_sbo4W9ze3s)

*A hackerek a sikerélményért, a saját rátermettségük bizonyításáért vagy leggyakrabban pénzért szegik meg a szabályokat és a törvényt. A zaklatókat szerintetek mi motiválja, amikor másokat piszkálnak és megszégyenítenek?*

*(düh, bosszú, irigység, hatalomvágy, rosszindulat stb)*

Mindaz, amit felsoroltatok, csupa negatív emberi tulajdonság, így leszögezhetjük, hogy a zaklatók nem lehetnek követendő példa senki számára, egyáltalán nem cool közéjük tartozni! Ne engedjetek a megfelelési kényszernek és a csordaszellemnek! Már azzal is közreműködsz részesévé válsz a zaklatásnak, ha tudsz róla, de nem teszel semmit a bántalmazás ellen. Ne nézzetek félre, ne legyetek közömbösek a szenvedő fél iránt, hiszen bárkiből válhat áldozat. Ha kiálltok a zaklatott diáktársatok mellett, lehet, hogy a zaklatók is meggondolják magukat.

*Előfordul, hogy beszóltak neked egy online játék közben, vagy hogy azért kellett kilépned egy online játékból, mert valaki nem hagyott békén?*

**Milyen következményekkel járhat a zaklatás, ha nem tesztek semmit ellene?**

Csakúgy, mint a többi bántalmazási forma, a cyberbullying aláássa az önbizalmat, az önértékelést, súlyos szorongást okoz a zaklatás elszenvedőjének. A folyamatos stresszhelyzet miatt nem élheti a megszokott, hétköznapi életét, kihatással lehet az iskolai teljesítményére, mentális, pszichés betegségekkel és valódi fizikai tünetekkel is járhat. Legvégső esetben akár öngyilkossághoz is vezethet, ha valaki nem kap időben segítséget.

 *Hallottatok már Momo- ról? Mit tudtok róla?*

[Momo](http://www.blikk.hu/aktualis/belfold/a-momo-nevu-internetes-horrorleny-miatt-lehetett-ongyilkos-a-15-eves-magyar-lany/j91362r) egy virtuális szörny, amely elsősorban a Whatsapp-on keresztül fenyeget. (Nemrégiben megjelent a népszerű, főleg fiatal gyerekek által játszott internetes játékban, a Minecraftban is)

A szörny horrorüzenetekkel zaklatja a kiszemelt áldozatokat, rémisztő hangokat, képeket, videókat vagy éppen a saját eszközükről lopott fényképet küld el nekik. Ezenkívül gyakran fenyegetések terhe mellett különféle feladatokkal bízza meg a rémült gyerekeket, például, hogy küldjék tovább az üzenetet, vagy akár csonkítsák meg magukat, illetve legyenek öngyilkosok. A helyzet komolyságát jelzi, hogy már halálos áldozatai is vannak, mégpedig a korosztályotokból.

A jó hír, hogy Momo nem létezik csak a virtuális térben, fizikailag nem tud és nem is akar érintkezni veletek. Mint minden virtuális lény egy gombnyomással, letiltással „elpusztítható”.

A legjobb védekezés, a megelőzés, vagyis, ha nem keresitek a vele való kapcsolatot, ha pedig ő keres benneteket, nem álltok szóba vele és azonnal jelzitek a szüleiteknek a zaklatást.

*Mit tennétek, ha titeket zaklatnának? Kihez fordulnátok segítségért?*

* Ne válaszolj a zaklatóknak! Gyakran csak a reakcióra kíváncsiak; ha figyelmen kívül hagyod őket, akkor elveszíthetik az érdeklődésüket.
* Blokkold a zaklató üzeneteit! Cseten, e-mailben vagy közösségi oldalakon letilthatod a zaklatótól érkező üzeneteket.
* Tartsd meg az e-maileket és egyéb üzeneteket, lehet, hogy ezeket valamikor bizonyítékként tudod majd felhasználni.
* **Nem vagy egyedül! Kérd bátran a szüleid, tanárod, vagy más megbízható felnőtt segítségét!**

Sok gyerek még a közvetlen környezetével sem meri megosztani félelmeit, mert szégyelli, ami vele történik, és úgy gondolja, hogy a segítségkéréssel csak a saját helyzetét nehezíti.

A felnőttek, akikben megbíztok - elsősorban a szüleitek - útmutatást, támogatást nyújthatnak, akkor is, ha online kerültök bajba. Természetesen érthető, hogy nehéz elmondani, ha akarva vagy akaratlanul bajba keveredtetek, de biztosak lehettek benne, hogy segítségetekre lesznek egy-egy nehéz helyzet megoldásában.

Bizonyos esetekben előfordulhat, hogy nem fordulhattok a szüleitekhez, ilyenkor keressetek egy általatok jól ismert, megbízható felnőttet (pld tanár, edző stb), akivel megoszthatjátok a problémátokat.

*Hogyan kezdenétek egy olyan beszélgetést a szüleitekkel, ahol be kell vallanotok, hogy bajba kerültettek a neten?*

*Példaként felhozhatók az alábbiak:*

"Tévedtem – olyan képet küldtem magamról, amit nem kellett volna, és most mások is látták."

"Megértem, hogy ideges vagy. Megpróbálom kitalálni, hogy mit tegyek - ezért beszélek veled.

"Érzem, hogy nincs rendben, amit tettem, és nem tudom, mit tegyek."

Három dolgot szeretnénk, ha mindenképpen elvinnétek magatokkal a mai beszélgetésből:

* Mindig figyeljetek adataitok biztonságára!
* Ne feledjétek, ha bajban vagytok, bátran kérjetek segítséget szüleitektől, vagy profi szakemberektől az Unicef help appján, vagy a 116-111-es Kékvonalon.
* Az internet sok csodát, lehetőséget rejt, használjátok felelősséggel és tudatosan!

**A ti generációtok beleszületett az internet világába, ami korlátlan lehetőségeket biztosít számotokra. Rajtatok múlik, hogy ne az időt pocsékoljátok el a kütyükkel, hanem arra használjátok, hogy a való világot jobban megismerjétek és kiteljesítsétek általuk.**