



## INTERNET ÉS BIZTONSÁG

### KÖZÉRTHETŐEN AZ INTERNETRŐL ÉS ANNAK VESZÉLYEIRŐL-SEGÉDLET

*Ezt az előadási anyagot a **Nemzetközi Gyermekmentő Szolgálat Magyar Egyesülete** készítette az Európai Unió **BIK NET** (Better Internet for Kids) projektje keretében. Célja, hogy minden iskola, nevelési és művelődési illetve egyéb intézmény számára elérhetővé tegyen egy, a biztonságos internetezés alapszabályait bemutató előadást. Annak érdekében, hogy a témában esetleg kevésbé járatos pedagógusok, könyvtárosok, intézményvezetők stb. is minden további nélkül megtarthassák az előadást, közrebocsátjuk ezt a segédletet is, mely az előadás egyes diáihoz tartalmaz rövid magyarázatokat, megjegyzéseket. Érdeklődni: [sjp@gyermekmento.hu](mailto:sjp@gyermekmento.hu)*

*Biztonságos internetezést kívánunk!*

3. dia

Az itt felsorolt témákról lesz szó.

4. dia

A mindennapi életünkhöz már teljességgel hozzátartozik az internet, és használata nélkül az élet több területén is hátrányt szenvednénk, gondoljunk csak a napi kapcsolattartás, információgyűjtés, hivatalos ügyintézés, szórakozás stb. színtereire. A világ ott van előttünk egy karnyújtásnyira, azonban ha egy kicsit naivabb vagy, esetleg kevésbé vagy járatos a netezésben, akkor számodra veszélyt is jelenthet.

5. dia

Bármelyik területét is használod az internetnek, veszélybe bárhol kerülhetsz. Akár böngészel, akár levelezel, vagy csetelsz, esetleg letöltesz. Körültekintő internetezéssel és a megfelelő biztonsági beállításokkal ezek azonban megelőzhetőek!

6. dia

Az internet egy világméretű hálózat, hálózatok összessége, amely a Földet körülöleli.

7. dia

Bárhonnan is netezel, veszély leselkedhet rád. Teljesen mindegy, hogy az iskolából, otthonról, egy internet kávézóból vagy mobilról tolod a netet, ha nem vagy kellőképpen felvértezve tudással, akkor könnyen pórul járhatsz.



#### 8. dia

Számítógépünk védelme a tűzfal és a vírusirtó program használatánál kezdődik, valamint hogy ezek a programok mindig a legfrissebb verziójukban legyenek jelen a gépünkön. Ne feledd! A számítógép olyan, mint egy ház, aminek a bejáratai megnyílnak, vagy bezáródnak, attól függően, hogy éppen mit csinálsz az interneten.

#### 9. dia

Megfertőződni nagyon könnyű. Nem csak hordozható médiáktól, hanem internetes oldalaktól, spam-ektől, felbukkanó ablakokra való kattintástól is megfertőzheted a gépedet.

#### 10. dia

A legfontosabb tényező mégis a saját tudásunk, mert a gép nem tud dönteni helyettünk. A döntéseket mindig nekünk kell meghozni, és ha tudatlanságból rosszul döntünk, anyagi vagy erkölcsi károkkal szembesülhetünk.

#### 11. dia

Általában a gyerekek ezt a négy fő területet használják. Beszüljünk is róla.

#### 12. dia

Az e-mailezés az egyik leggyakrabban használt szolgáltatása a világhálónak. Az e-mail cím készítésekor a kukac előtt álló részt mi választhatjuk meg, mi magunk találunk ki ide valamilyen karaktersorozatot, ez lesz a felhasználónevünk, a kukacot és az utána álló részt, pedig az alkalmazás automatikusan hozzáteszi. Természetesen, mint egy jó lakat, jelszó védi a postaládánkat.

#### 13. dia

Mikor biztonságos egy jelszó? Nem ajánlatos a családtagok, háziállat, születési dátum használata, hiszen ezt mások is ismerhetik. Lehetőleg ne forduljon elő szótarban sem, tehát minél értelmetlenebb, annál jobb. Kerüljük a túl egyszerű jelszavakat: 12345, abcde stb. Ugyanazt a jelszót ne használjuk több területen, minden internetes dolgunkhoz külön jelszó legyen, hiszen ha azt az egyetlen feltörnek, mindent feltörnek vele. Legalább 7 karakter hosszú legyen, és a betűk mellett számokat és különleges jeleket is tartalmazzon. Bizonyos időközönként változtassuk meg a jelszót, s ha valamihez gyárilag kapunk, azt rögtön.

#### 14. dia

Ezek a leggyakoribb jelszavak, amiket véletlenül se használjatok!

#### 15. dia

Nézzünk 3 egyszerű példát arra, hogyan lehet könnyen biztonságosabb jelszavakat kitalálni. Az egyik módszer, hogy veszünk egy hosszabb értelmes szót, és csak kétkarakterenként használjuk fel, így lesz belőle értelmetlen jelszó, ami már szótarban sem fordul elő. A másik lehetőség, hogy megjegyzünk egy könnyű mondatot, és csak a szavak kezdőbetűit tesszük egymás mellé jelszóként. A harmadik, hogy a jelszavunk egy-két karakterét lecseréljük egy másik karakterre, ami ránézésre vagy kiejtésre hasonló.



16. dia

Nézzük meg, hogy egy ismeretlen személy hogyan próbál rájönni a jelszavunkra. (videó)

17. dia

Jelszavunkat soha ne adjuk kölcsön, mert mások írhatnak a nevünkben levelet, válaszolhatnak, törölhetnek; ha mégis ennyire meggondolatlanok voltunk, rögtön változtassuk meg! A kéretlen leveleket rögtön töröljük, a spamekre ne reagáljunk semmilyen módon sem, mert még több ilyen levelet fogunk kapni és a postaládánk ezek gyűjtőhelyévé válhat. Ha az említett 2 hibát elkövetjük, végső megoldásként ott az új e-mail cím készítésének lehetősége. Az ismeretlen helyről érkező leveleket szintén töröljük, mellékletüket ne nyissuk meg, vírusokat tartalmazhatnak. Ha mégis ebbe a hibába estünk, futassuk a vírusirtót!

18. dia

Így is lehet spam-et szűrni.

19. dia

Két dolgot tehetünk a probléma kiküszöbölésére: olyan levelezőrendszert használunk, amelyik rendelkezik SPAM szűrővel, valamint több e-mail címünk legyen. 3 mindenképp ajánlatos: 1 a hivatalos levelezésekhez, 1 a családon belül (rokonokkal), 1 internetes regisztrációkhoz, közösségi oldalakhoz stb.

20. dia

Ugyancsak hasznos megoldás, hogy a szabványos e-mail cím megadása helyett, ha van rá lehetőségünk, úgymond csak szavakkal írjuk le, vagy akár a saját honlapunkon így adjuk meg az e-mail címünket. Erre az e-mail címeket szabványos alakban felismerő és begyűjtő kémprogramok miatt van szükség.

21. dia

Számodra ismeretlen, esetleg érthetetlen magától felbukkanó ablakkal NE hagyd magad „eltéríteni”! Használd a Kedvencek mappát! Nem kell mindig keresni, időt takaríthatsz meg vele. Ha információt keresel, legalább 3 különböző oldalon nézz utána! Az internetre bárki, bármit feltehet!

22. dia

Egy-egy meggondolatlan letöltés komolyabb anyagi terheket is róhat ránk, ezért fontos az alapos körültekintés. A veszély abban is rejlik, hogy nem tudunk ellenállni ingyenesnek hirdetett tartalmaknak (csengőhangok, háttérképek stb.), melyek megrendelése igen sokba kerülhet. Ezen felül a gépünkre töltött adatok akár károsak is lehetnek. Éljünk a gyanúval, hogy ha egy egyszerűnek tűnő letöltéshez túl sok információt kérnek tőlünk, lehet, hogy bizalmas adatainkat akarják megszerezni. A felbukkanó POP-UP ablakok ajánlataira, pedig soha ne reagáljunk, zárjuk a piros X-szel!

23. dia

Ha már letöltöttünk valamit a számítógépünkre, tartsuk be a következő 3 lépést: mentés, vizsgálat, megnyitás!



24. dia

A chat-elés remek szórakozás és időtöltés. Könnyen tudunk bárkivel kapcsolatot teremteni és azt fenntartani, azonban a kellő óvatosság nem árt. Sosem tudhatjuk, hogy a mások oldalon valójában ki van.

25. dia

A chat-es programokba más is beleolvashat, ezért személyes információkat még véletlenül se adjunk ki magunkról. A chat alkalmazásokkal nem csak beszélgetni lehet, hanem adatokat is küldeni. Ezért fennáll a veszély, hogy kártevők kerülhetnek a gépre. Az interneten nem mindenki az, akinek mondja magát. Nem szabad mindent elhinni, amit a másik és mond. És sose találkozz az interneten megismert idegennel!

26. dia

Néhány alapvető chat szabály:

- Legyél óvatos, ahogy az utcán is!
- Őrizd meg a magánjellegű információkat, ne mondj magadról túl sokat!
- Tartsd be a netikettet: jó modort (úgy bánj másokkal, ahogyan szeretnéd, hogy ők bánjanak veled)!
- Sértő üzenetekre ne válaszolj (de mentsd el, mert bizonyíték lehet, ezután szólj felnőtteknek)!

Nagyon fontos, mindig kérd bátran felnőtt segítségét, ha elbizonytalanodtál vagy kérdésed van!

27. dia

A következő kisfilm azt mutatja be, hogy egy idegen hogyan próbál másnak mutatkozni a neten, mint aki valójában. (videó)

28. dia

Igazából tökéletes védelem nem létezik az ilyen jellegű csalások ellen, de ha néhány alapvető szabályt megjegyzünk, és azokat be is tartjuk, akkor már képesek vagyunk hatékonyabban védekezni a támadások ellen.

- Ne bízzunk meg egy bejegyzésben, üzenetben vagy meghívóban csak azért, mert az egy ismerősünktől érkezett. Őt is becsaphatták, fiókját feltörhették, vagy kártevő fertőzhetette meg a számítógépét.
- Vigyázzunk az ingyenes ajánlatokkal, különösen, ha cserébe csak lájkot vagy megosztást várnak el tőlünk.
- Ha valamit látatlanban előre kell lájkolni, NE tegyük. Kérdéses vagy gyanús esetekben pedig keressünk rá az interneten, hátha már egy ismert csalással akarnak rászedni bennünket.
- Ha egy "shocking" vagy "must see" Facebook videót csak akkor lehet megnézni, ha előtte lájkolni vagy csatlakozni kell egy közösséghez, ne tegyük!
- Sose kattintsunk olyan linkre, amely mehökkentő tartalmat ígér, mint például "Amy Winehouse pictures!" vagy "Osama bin Laden death video!", vagy az egónkat célozza meg, mint például "Az emberek 98 %-a nem tudja 17mp-nél tovább nézni a videót!" stb.
- Ha egy Facebook-videót csak akkor lehet megnézni, ha előtte engedélyezni kell egy ismeretlen alkalmazás telepítését, amely természetesen hozzá akar férni az üzenőfalhoz, ismerőseinkhez, személyes adatainkhoz, ne engedélyezzük.
- Sose kattintsunk olyan alkalmazásra, amely azt ígéri, hogy megmutatja kik és hányszor nézték meg a Facebook profilunkat, fotóinkat!



29. dia

Végül, de nem utolsó sorban: minden kattintás előtt érdemes végiggondolni, megéri-e kiszolgáltatni személyes adatainkat ismeretlen személyeknek, csak azért, hogy meg tudjuk kik nézték meg a fotóinkat, melyik drágakő illik hozzánk a legjobban, mi az indián nevünk, előző életünkben kik vagy mik voltunk, és így tovább.

30. dia

Az idegen a neten is idegen. Légy óvatos, ne kommunikálj túl sokat magadról, a webkamerát ne kapcsol be idegen kérésére. Ha valaki kényes, ízléstelen, esetleg szexuális jellegű kérésekkel próbálkozik, akkor azonnal szakítsd meg a kapcsolatot és szólj felnőtteknek.

31. dia

Ha már beszélgetésbe kezdted, akkor légy óvatos. Használj fantázianevet, mindenki ezt csinálja. Ne áruld el az életkorodat, lakcímedet, telefonszámodat. Sose mondd el, hogy honnan netezel! Ha nem tetszik a beszélgetés menete, ne folytasd, inkább szólj felnőtteknek. Érdemes az üzeneteket elmenteni, gondolva a későbbiekre (bizonyítékként szolgálhatnak).

32. dia

Mielőtt fényképet töltesz fel magadról az internetre, gondolkodj el rajta, hogy szüleid barátaid hogyan reagálnának erre. Ami ma viccesnek tűnik, az a jövőben teljesen más lehet. Együtt kell élned minden fényképpel, amit valaha feltöltöttél, és vállalnod kell rajta magadat. Ha erre képtelen vagy, akkor ne töltsd fel.

33. dia

Egy rossz pillanatban készült kép jó időre megkeserítheti az életedet! (videó)

34. dia

A virtuális zaklatás mások szándékos és tartós fenyegetése, sértegetése, megalázása a digitális médiák felhasználásával.

Elsődleges színtere az internet, ezen belül a közösségi hálózatok, chat szobák, e-mail üzenetek, blogok és fórumok. További színtere a mobiltelefon, melynek használatával zaklató SMS-ek vagy idegesítő telefonhívások, esetlegesen kellemetlen fényképek és videók tehetik tönkre mindennapi életünket. Zaklató tartalmú üzeneteket, SMS-eket, e-maileket, fórum és blog bejegyzéseket mentsd el, hogy történeted hihető legyen. Ha nem tudod elmenteni, készíts képernyőképeket, például egy kellemetlen fényképről, vagy beszélgetésről. Blokkold a zaklatót! Nagyon sok internetes alkalmazásban lehetőséged van arra, hogy a nem kívánatos személyeket letiltsad, blokkold. Mindig kérj segítséget! Nem ciki mástól segítséget kérni.

35. dia

A szavak sokkal jobban fájnak, és nagyobb sebet ejtenek, mint gondolnád. Ha valaki zaklat, blokkold és jelentsd. (videó)



36. dia

A digitális térben mindenki hagy nyomot maga után. A szolgáltatók minden tevékenységünket, kattintásunkat naplózzák. Nem lehet elbújni csak úgy a neten, ezért nyugodtan fordulj a rendőrséghez, ha zaklatnak.

37. dia

Érdemes az IMEI számot feljegyezni, hiszen ha ellopják vagy elveszted a telefonodat, akkor könnyebben megtalálható lesz, ugyanakkor minden funkcióját le lehet tiltatni távolról. Fotózáskor fontos tudnod, hogy bizonyos helyeken nem illik vagy akár tilos fotózni; valamint magunk is dönthetünk, hogy lefotózzanak vagy sem.

38. dia

Néhány mobil szabály, amit érdemes észben tartanod:

- A rejtett szám hívásokkal óvatosan bánj.
- Az országon kívülről érkező hívásokat ne fogadd és ne is hívd vissza. Könnyen csalók áldozatává válhatsz.
- A fenyegető, ijesztő, durva sms-eket mentsd el és szólj felhőttnek.
- Kellemetlen, durva fotókat, videókat ne továbbítsd és ne is tárold a mobilodon.
- Mielőtt szervizbe viszed a telefonodat ments ki mindent memóriakártyára, majd töröld a telefonban lévő képeket és videókat.
- Ne közlekedj bekapcsolt bluetooth-szal, az ismeretlen kapcsolódásokat utasítsd vissza.

39. dia

Könnyen válhatunk SMS csalások és vámpír-szolgáltatások áldozataivá egyetlen ártatlannak tűnő vagy nagy nyereséggel kecsegtető SMS elküldésével, esetleg multimédiás tartalom letöltésével, mely ezeket aktiválja. Érdemes mindig átgondolni, hogy mihez is adunk hozzáférést, amikor a mobilszámunkat adjuk meg egy webes felületen.

40. dia

Böngészés során gyakran bukkannak fel ehhez hasonló, mesés nyereséggel kecsegtető ablakok, melyek a telefonszámunkat várják tőlünk. Abban a pillanatban, amint ezt megadjuk, egy szerződést kötöttünk, s hamarosan jelentős összegeket vonnak le telefonunkról, s erről csak egy apró betűs rész tájékoztat, vagy maga a tájékoztatás is félrevezető. Ezért mindig legyünk óvatosak, ha valamilyen nyereség ürügyén a telefonszámunkat kérik.

41. dia

Amennyiben vámpírszolgáltatás áldozatává váltál, akkor szüleiddel menj be saját mobilszolgáltatódhoz, és kérd az emelt díjas szolgáltatások törlését. Ha netán megrendeltél valamit a mobilodra és tudod a számot, akkor küldd utána a STOP szót, és a szolgáltatás attól a naptól kezdve megáll.

42. dia

Sokan használnak manapság okostelefont, azonban gyakran felelőtlenül teszik. Az itt felsoroltak közül a legfontosabb a helymeghatározás (google koordináták) kikapcsolása, hiszen senkinek semmi köze, hogy honnan használom a telefont. Ezenkívül érdemes a QR kódok linkjeinek előzetes ellenőrzése, hiszen a kód mögé bármi eldugható, akár káros weboldalra mutató link, szexuális, gyűlölködő tartalmú honlapok stb.



43. dia

Az okostelefonok állandó használata könnyen függőséghez vezethet! Erre hívja fel a figyelmet ez a reklám. (videó)

44. dia

Bármilyen probléma esetén, amit nem szeretnél sem a szüleiddel, sem a tanároiddal megbeszélni, nyugodtan fordulhatsz a Kék Vonal munkatársaihoz. Ők tudnak neked segíteni. Ha netán káros vagy illegális tartalommal találkozol a neten, azt a <http://biztonsagosinternet.hu> weboldalon tudod bejelenteni.

45. dia

Néhány hasznos és megbízható weboldal, amit érdemes felkeresni.

