Szülõi útmutató

Gyermekeink on-line biztonsága

ins@fe

A UPC Magyarország támogatásával
www.upc.hu

TARTALOM

A. Használati utasítás

Ha egy évre tervezel, ültess rizst.
Ha tíz évre tervezel, ültess fát.
Ha egy életre tervezel, nevelj gyereket.

Kínai mondás

Kedves Szülők/Nevelők!

Az alábbi e-biztonsági oktatási csomag 6 és 12 év közötti gyerekek családjának szól. Abból a meggyőződésből készült, hogy az új technológiáknak nem elválasztaniuk, hanem egyesíteniük kellene a generációkat. Az Insafe, a pán-európai hálózat nemzeti kapcsolati központjainak tapasztalataira alapozva próbálja a biztonságosabb internetezést tudatosítani mindenkiben. A UPC támogatta ennek az e-biztonsági csomagnak a fejlesztését és létrejöttét.

A játszótéren való játék és az utcai átkelés is veszélyes lehet, ha nem vagyunk körültekintőek, és ugyanígy az internet és a mobil technológiák is veszélyt jelenthetnek az elővigyázatlan felhasználó számára. Szerencsére számos, a web előnyeiről, veszélyeiről és a szörfölésről szóló tanító eszköz áll az internet-felhasználók rendelkezésére.

Az oktatási csomag használatával segíthetjük gyermekünket abban, hogy biztonságos és hatékony módon tanulja meg használni az internetet. Ez a csomag szórakoztató és érdekes formában,

több mint 50 biztonsági tippet és gyakorlatot kínál a gyerekek tanítására az e-biztonság területén. A csomag tartalma a következő:

- Két e-biztonsági füzet: családi szórakozás és szülői útmutató résszel;
- Aranyszabályok;
- Családi bizonyítvány;
- Címkék;
- 12 szituációs kártya, melyeket a gyerekeknek kell kivágni.

A színkódolású családi és szülői füzetek négy alapvető e-biztonsági témát hangsúlyoznak: Biztonság, Kommunikáció, Szórakozás & Letöltés és Virtuális erőszakoskodás. A szülői füzet referenciául szolgál a családi szórakoztató részhez: háttér-információkkal szolgál, magyarázatot fűz a feladatokhoz, illetve tartalmazza a gyakorlatok és a szituációs kártyák javasolt megoldásait.

A családi füzetet érdemes a szülőknek a gyerekekkel együtt használni. A négy témát a két kamasz fiatal, Alex és Zeta, valamint szüleik és az IT zseni, Hedvig történetein keresztül közelítjük meg. Minden fejezet oktatási feladatokat tartalmaz, beleértve az online gyakorlatokat, kvízeket, az aranyszabályokat és a hasznos linkeket is.

Olvassuk el hangosan a történeteket a gyerekekkel és oldjuk meg közösen a feladatokat. A fejezetek végén a megfelelő szituációs kártyák olyan vitatémákat kínálnak, amelyek segítségével jobban megérthetjük a témát és elmélyíthetjük tudásunkat.

Ha gyerekeink sikeresen eljutottak a végéhez, jutalmazzuk meg őket és írja mindenki alá a családi bizonyítványt, majd beszéljük meg az aranyszabályokat. A végén díszítsék ki a gyerekek a füzetet különböző emotikon címkékkel.

Minden visszajelzés nagyon fontos. Kérjük, ha tehetik, írják meg véleményeiket és kérdéseiket a helyi Insafe információs központnak. Önnek és az egész családjának jó szórakozást kívánunk az internet megszelídítésében!

Biztonságos szörfölést mindenkinek!

Aláírás

ins@fe

B. Útmutató szülőknek és nevelőknek:

1. A Biztonság Biztonságot szül

SZÁMÍTÓGÉP @ LAKÁSBAN

Az otthoni számítógép az egész család számára egy nagyszerű oktatási és kikapcsolódási lehetőség lehet. Sokat segítünk a fiatal családtagoknak a biztonságos internetezésben, ha a gépet a lakás központi helyén helyezzük el és megszabjuk a feltételeket, hogy hogyan és mennyit használhatják a gépet.

Ne felejtsük el, hogy gyerekeink a barátaiknál, internetkávézókban stb. is csatlakozhatnak a világhálóra. Ezért fontos, hogy együtt alapozzuk meg azokat a biztonságos viselkedési szabályokat, melyeket bárhol és bármikor alkalmazhatnak majd.

A SZÁMÍTÓGÉPÜNK BIZTONSÁGA

A potenciális veszélyek és egyszerű megoldások elsajátításával megteremthetjük a biztonságot. A megoldások között említhetjük a hasznos technológiai eszközöket, illetve a felhasználók józan eszét. Mint ahogy minden más, a józan ész is fejlődik korral és tapasztalattal.

Veszélyforrást jelenthet mindaz, ahogyan mi és gyerekeink otthon a számítógépet általában használjuk: pl. **memóriakártyák**, vagy **CD-ROM**ok **használata**, **csatolt fájlok** megnyitása, **fájlok letöltése**. Ezeket a veszélyeket leginkább az olyan rosszindulatú számítógépes programok (malware) jelentik, melyek szándékosan a számítógép tönkretételére, a személyes adatok megszerzésére szolgálnak, illetve nem kívánt reklámokkal látnak el minket.

A gyerekeknek magyarázzuk el a malware típusait: **vírusok**, **férgek**, **trójai lovak** és **kémszoftverek**, és tanítsuk meg nekik a fertőzött számítógép tüneteinek felismerését. Megtanulhatják, hogyan előzhetők meg a fertőzések azzal, hogy mindig naprakész **anti-vírus** és **anti-kémszoftver** programmal ellátott számítógépen keresztül csatlakoznak az internethez. Tanácsoljuk nekik továbbá, hogy legyenek mindig óvatosak, ha megnyitnak egy ismeretlen küldőtől érkezett e-mailhez csatolt fájlt, ha programokat töltenek le az internetről, illetve USB-t vagy CD-ROM-okat használnak.

KÜZDELEM A SPAM ELLEN

Az interneten keringő e-mailek 80%-a **spam** (nem kívánt e-mail), mely könnyen hatással lehet gyerekeinkre. A **neten levelezőcsoport**, **chat** oldal, közösségi fórum, társadalmi kapcsolatépítés vagy akár egy online formanyomtatvány használata során nem szándékosan közzétett **e-mail cím** spam-et eredményezhet. Az e-mail címeket az internetről speciális szoftverek gyűjtik össze, hogy olyan levelezőlistákat hozzanak létre, melyek hatalmas mennyiségben terjesztik a spameket. Az ilyen tevékenységben résztvevő cégek székhelyei általában olyan helyen találhatók, ahol a nem kívánt e-mailre vonatkozóan nincs jogszabály!

A spam e-mailek leggyakrabban pornográf, gyógyszerekkel kapcsolatos, kétes pénzügyi stb. információkat tartalmaznak. Ezen túlmenően a spam rosszindulatú programok forrása is lehet. A legtöbb estben a spam e-mailek tisztességtelen szándékkal érkeznek. Az alábbi tanácsok segíthetnek családunk megvédésében:

- Használjunk "**spam szűrőt**". Az elektronikus levelezési szolgáltatók általában az e-mail programban működtethető anti-spam lehetőségeket bocsátanak rendelkezésre. Bővebb információért vegyük fel a kapcsolatot a szolgáltatóval. Ellenőrizzük rendszeresen a **szemét és spam** mappákat, hogy nem került-e közéjük ártalmatlan e-mail. A technológia sem tévedhetetlen.
- Tanítsuk meg gyerekeinket arra, hogy ismeretlenek e-mailjeit ne nyissák meg. A spam tartalma mindig ígéretesnek tűnik vagy megtévesztő csatolt fájlt tartalmaz. Mutassuk meg a gyerekeknek, hogyan lehet az e-mailt küldő személyt "blokkolni" illetve kérjük meg őket arra, hogy a gyanús e-maileket egyszerűen töröljék.

SZÖRFÖLÉS A NETEN

Még az egészen kis gyerekek is profitálhatnak az interneten történő szörfölésből, ha szórakoztató, illetve oktatási célú **honlapokat** látogatnak. Ugyanakkor az internet sokszor korosztályra való tekintet nélkül kínál mindenféle tartalmat.

A keresőprogramokkal nagyszerűen találhatunk rá az adott témára. Mivel azonban a keresés kulcsszavakon alapul, a nem kívánt tartalmat is egyszerű megtalálni. Egy ártatlanul csengő kulcsszóval rábukkanhatunk kevésbé ártatlan honlapokra is, amelyek valóban tartalmazzák a keresett kulcsszót. Az alábbi tippekkel segíthet gyerekének abban, hogy biztonságosabban szörfözhessen az interneten:

- Hozzunk létre egy olyan speciális felhasználói profilt a gyermekünk részére az általunk használt **operációs rendszerben**, (pl.: Windows, Linux, Mac OS), melyen **szülői felügyelet működtethető;**
- Ellenőrizzük a szülői felügyeleti lehetőségeket az **internetböngészőben** és a keresőprogramban. Győződjünk meg arról, hogy ismerjük ezen eszközök **családi beállításainak** lehetőségeit;
- Felügyeletünk alatt álló gyerekeknek javasoljuk a gyerekbarát **keresőprogram** használatát. Erre példa a http://kids.yahoo.com, http://www.askforkids.com honlap;
- Mentsük el a gyerekek által leggyakrabban használt honlapokat a **Kedvencek** mappába (böngésző lehetőség). Ezáltal lehetővé tesszük számukra, hogy kedvenc **net**-helyeiket keresőprogramok nélkül érjék el.

A browser és a keresőprogram szülői felügyeleti lehetőségein túlmenően kiegészítő **szűrőt** is használhatunk, vagyis olyan szoftvert, mely megvédi a kicsiket a nem megfelelő tartalmú honlapoktól. Kérjünk tanácsot szakértőtől vagy keressünk az interneten **kísérleti szoftvereket**. Ne felejtsük el, hogy semmi nem helyettesítheti a szülői figyelmet és a gyerekekről való gondoskodást. A technikai eszközök nem tévedhetetlenek és a józan ész nélkül a biztonság hamis látszatát kelthetik.

A szűrésre használt szoftver olyannyira korlátozó jellegű lehet, hogy az ártalmatlan tartalmat is kiszűri. Megakadályozhatja gyermekünket például a II. Világháborúval kapcsolatos leírások keresésében, ha az esetleg erőszakot ábrázoló vagy leíró honlapokhoz vezetne el. Minden szűrőt, amit be lehet kapcsolni, ugyanúgy ki is lehet kapcsolni, ha egy leleményes gyerek, aki ért a nyomok eltüntetéséhez a saját útját szeretné járni. Erre csak akkor jöhetünk rá, ha magunk is megtanuljuk használni a számítógépet és a szoftvert.

Látogassunk el az Európai Bizottság által támogatott SIP-Bench honlapra (lásd a hasznos címek között), amely 30 szülői felügyeleti és anti-spam eszközzel kapcsolatos tesztet tartalmaz arra vonatkozóan, hogy azok mennyire hatékonyan képesek megvédeni a 6 és 16 év közötti gyerekeket az interneten közzétett különböző alkalmazások - **böngésző**, emailezés, **fájltovábbítás**, társalgás és **azonnali üzenetküldés** – rosszindulatú tartalmaitól.

A **káros tartalmak** elkerülése mellett tanítsuk meg gyerekeinket arra is, hogy ne higgyenek el mindent, amit az interneten látnak, vagy olvasnak. A családi szórakoztató füzetben azt tanácsoljuk, hogy amennyiben online információra van szükség, érdemes legalább 3 honlap tartalmát összehasonlítani. Az információ forrását se felejtsük el megemlíteni, akkor is, ha iskolai dolgozatról van szó.

ARANYSZABÁLYOK A SZÖRFÖLŐ GYEREKEK SZÜLEINEK

• Győződjünk meg róla, hogy számítógépünk **tűzfallal**, anti-vírus és anti- kémszoftverrel van védve. Ez utóbbi legyen naprakész, folyamatosan frissített és vegyük komolyan a **figyelmeztetéseket**. Nézzünk utána, hogy az internet szolgáltató (ISP) milyen használható anti-vírus és anti-kémszoftver eszközöket kínál;

• Használjunk spam-szűrőt az e-mailezés során és lehetőleg ne tegyük közzé e-mail címünket a neten. Kerüljük az ismeretlen feladótól érkező e-maileket és megnyitás előtt **ellenőrizzük** a csatolt fájlokat;

• Maximalizáljuk a szülői felügyeleti lehetőségeket az operációs rendszerben, az internetböngészőben, a keresőben és az e-mailezés során. Hozzunk létre különálló **felhasználói profilt** gyerekeinknek. Győződjünk meg arról, hogy a biztonsági beállítások a legmagasabbra vannak állítva (nézzük meg a "Opciók" menüt a böngészőben);

• Fontoljuk meg további szűrő szoftverek alkalmazását;

• Forduljunk szakértőhöz, ha gépünk furcsán kezd viselkedni, mert lehet hogy fertőzött. Általában az internet -zolgáltató is segít a szülőknek;

• Használjuk a nemzeti internetes **forródrótot** (ld. Hasznos linkek) ha nem kívánt tartalmakkal találkoztunk a neten;

• Ha lehet, legyünk a gyerekünk közelében, miközben szörföl. Remek lehetőség a beszélgetésre, illetve a bizalom erősítésére. Tegyük érdekfeszítővé az együtt tanulást;

• Ne feledjük, ezek a biztonsági tanácsok nekünk és a gyerekeinknek szólnak. Bátorítsuk őket, hogy ha furcsa dolgot észlelnek, rögtön mondják el.

HASZNOS LINKEK

Az alábbi oldal a Barátságos Internetről szól gyerekeknek, szülőknek, pedagógusoknak. Megtanítja a biztonságos netezéshez szükséges alapvető szabályokat és figyelmeztet a veszélyforrásokra. *http://www.baratsagosinternet.hu*

Ha aggodalom nélkül szeretnénk szörfözni, a tudás kulcsfontosságú: jó, ha ismerjük a kockázatot, és tudjuk azt is, hogyan védhetjük meg magunkat. Ehhez nyújt segítséget a Hun-CERT védelmi eszközökkel kapcsolatos leírása, amely az alábbi linken keresztül érhető el: *http://www.cert.hu*

Biztonsággal kapcsolatos hasznos tanácsokat találhatunk az alábbi honlapon is: *http://www.bigyoo.hu*

Ha elbizonytalanodunk egy illegális tartalmat illetően, jelezhetjük a magyar forródrót szolgálatnak is: *http://www.internethotline.hu*

SIP-Bench
http://www.sip-bench.org

2. Kommunikáció ;-D

A PUZZLE RÉSZEI

Emlékszünk még, milyen fontos volt számunkra gyerekkorunkban a barátokkal való kapcsolattartás? Számos lehetőséget kínál az internet a barátokkal való találkozásra, új lehetőségeket az önkifejezésre és a kapcsolattartásra az e-mailen, a **fájl megosztókon** és a **blogokon** keresztül, valamint a társadalmi kapcsolatok építésére (pl. MySpace, Facebook, Hi5, Habbohotel stb). Napjaink tizenévesei a technológiát arra használják, hogy új dolgokat próbáljanak ki egy olyan térben, ahol úgy érzik, hogy egyedül vannak, távol a szülői felügyelettől.

A "Kommunikáció" fejezet megismerteti a szülőket és gyerekeket a **személyes adatok** és a **magánszféra** fontosságával, valamint a pozitív online kapcsolattartással, és az olyan kockázatok kezelésével, mint például az idegenekkel való kapcsolat. Az online magánszféra szorosan kapcsolódik az azonosító és a profil fogalmaihoz. Az azonosító segítségével érhetjük el az online szolgáltatásokat.

A valós világban a buszbérlet, a fitness-bérlet vagy bármilyen tagsági kártya tartalmazza személyes adatainkat. Hasonlóan működik ez az online azonosítók és szolgáltatások esetében is. Addig nem tudjuk egyiket sem használni, amíg meg nem adjuk személyes adatainkat a felhasználói "azonosítás céljából". Nagyon fontos, hogy megválaszthatjuk azt is, hogy milyen információt szeretnénk magunkról nyilvánosságra hozni, valamint azt is, hogy ezt az információt kivel szeretnénk megosztani.

A magánszféra védelme nem azt jelenti, hogy hazudunk a személyazonosságunkat illetően, hanem azt, hogy helyesen kezeljük az adatainkat és csak annyit mondunk el adott személynek magunkról, amennyi az illetőre tartozik. A fiatalok lelkesen beszélgetnek barátaikkal és alakítanak ki magukról képet online. Sokszor nem is sejtik, milyen következményei lehetnek annak, ha személyes adataikat közzéteszik.

PROFIL LÉTREHOZÁSA

Személyes adataink védelmének első lépése egy biztonságosabb profil létrehozása, megfelelő adatokkal és megfelelő biztonsági beállításokkal.

Hozzunk létre több e-mail címet a különböző online szolgáltatásokhoz. Az online társalgáshoz, az azonnali üzenetküldéshez, illetve a bloggoláshoz stb., javasoljuk gyerekeinknek, hogy egy semleges e-mail címet és **képernyő nevet** használjanak. Így a társalgó gyerek nem a teljes nevét használja az e-mail címben.

A **jelszavunkat tartsuk** mindig titokban. Próbáljuk megértetni velük, hogy személyes adataikat ne

osszák meg olyan barátaikkal, akik visszaélhetnek vele. Ugyanakkor beszéljük meg gyerekeinkkel azt is, ha felhasználói profiljaik ellenőrzése végett ismerni szeretnénk jelszavukat.

Ne feledjük profiljaink/azonosítóink személyes beállításait nyilvános helyett inkább titkos módra állítani. Ez lehetőséget biztosít annak eldöntésére, hogy azokat ki láthassa, és hogy kivel kommunikálunk. A privát profil az jelenti, hogy a kapcsolattartást mi határozzuk meg (**kapcsolatok**). Tanítsuk meg gyerekeinknek, hogy csak a valóságban már ismert emberek üzeneteit fogadják.

Ha a gyerekek chat-szobát látogatnak, ellenőrizzük, hogy:

- valós moderátorral történik-e mindez. A moderátor nélküli társalgás nem biztonságos;
- vannak-e olyan eszközök, melyek kiszűrik vagy letiltják a nem kívánt társalgót;
- a honlapon van-e **segítség** és **bejelentési** szolgáltatás bármely probléma felmerülése esetén;
- a szolgáltatás szabályai érthetően és jól láthatóan le vannak-e írva.

KÉPEK ÉS WEBKAMERÁK

A gyerekeknek meg kell érteniük, hogy a fényképük személyes adatuk, és hogy bármely digitális kép könnyen továbbítható és **manipulálható**. Ha egyszer már a számítógépen vagy a mobiltelefonon keresztül közzétettük, nagyon nehéz eltüntetni - örökké online maradhat a fotó! A webkamerákkal ajánlatos óvatosan bánni, olyannyira, hogy a gyerekek felügyelet nélkül ne is használják. Webkamerákat érintő chat eszközök és a **címjegyzék** használata kockázatos lehet. Csak olyan embereknek küldjünk személyes fényképeket, akiket jól ismerünk, és akikben bízunk – ha valaki más fotóját küldjük el, attól mindig kérjünk engedélyt. Ne engedjük, hogy gyerekeink szobájukban egyedül használják a számítógépet és a webkamerát.

KAPCSOLAT IDEGENEKKEL

Akikkel online megismerkedünk, azok nem mindig azok, akiknek mondják magukat. Tanítsuk meg gyerekeinket arra, hogy magánszférájukat ugyanúgy őrizzék meg, mint a valós életben. Ha megtanítjuk őket arra, hogyan viselkedjenek idegenekkel az utcán, miért ne követhetnék ugyanazokat a szabályokat az interneten is?

A gyerekek hajlamosak szoros barátságba kerülni online ismerősökkel, és olyanokban bízni, akiket nem is ismernek igazán, de akik érdeklődést és megértést tanúsítanak irányukban. Következésképpen késztetést éreznek arra, hogy személyesen találkozzanak velük, anélkül, hogy ezt elmondanák nekünk. A gyerekek gyakran nincsenek tisztában az ilyen találkozás rejtette veszély lehetőségeivel. Könnyen online **grooming áldozatává válhatnak**. A tanulmányok kimutatják, hogy sok gyerek egyedül találkozik online “barátjával” anélkül, hogy erről szüleit értesítené. Beszéljünk erről a gyerekekkel, hogy hasonló eset ne történhessen meg velük. A kommunikáció kulcsfontosságú.

NETIKETT

A Netikett a jó modorra utal az interneten, valamint arra, hogy úgy bánunk másokkal, ahogy mi szeretnénk, hogy velünk bánjanak. A gyerekek talán észre sem veszik, és véletlenül megbántanak valakit online. Sajnos sokan az internetet és/vagy a mobiltelefont használják mások bántalmazására, sértegetésére. Ezt hívjuk virtuális erőszakoskodásnak (cyberbullying), amely négyből egy gyereket érint. (ld. Bővebb információk részben a megfelelő fejezetet).

CHAT NYELV

A fiatalok a társalgáshoz közös nyelvet használnak, tele **emotikonnal** és **betűszóval**! Az alábbi táblázatban megismerkedhetünk ezekkel.

Társalgási betűszavak, bővebben a hasznos linkek részben:

121: one to one

AFK: away from keyboard

A/S/L: age, sex, location (or just "ASL")

BBB: bye bye baby

B4N: bye for now

BBL: be back later

BF: boyfriend or best friend

BFF: best friends forever

C: see?

Comp: computer

CU: see you

CUL: see you later

CYO: see you online

EGBOK: everything going to be ok

F2F: face to face

JJ: just joking

K: all right /ok

KFY/K4Y: kiss for you

KISS: keep it simple, stupid

KPC: keeping parents clueless

L8R: later

IRL: in real life

LMIRL: let's meet in real life

LOL: laughing out loud, lots of love

LY4E: love you forever

NE1: anyone

NP: no problem/ noisy parents

OIC: oh, I see

OLL: online love

PAL: parents are listening

G2G or GTG: got to go

<G>: grin

GFN: gone for now

GL: good luck

GM: good morning /good match

HAND: have a nice day

^5: High 5

H2G: have to go

HDOP: help delete online predators

IDK: I don't know

ILU/ILY: I love you / I like you

PAW: parents are watching

PIR: parent in room / people in room

POS: parent over shoulder

RL: real life

S^, S'UP: what's up?

TTYL: talk to you later

TY: thank you

WB: welcome back/ write back

WDYT: what do you think

WTGP: want to go private?

WYCM: will you call me?

Emotikonokat úgy hozhatunk létre, ha az írásjeleket és a betűket kombináljuk, lásd az alábbi táblázatot:

Mosolygós arc (orral vagy orr nélkül)	:) vagy : -) kettőspont, (kötőjel), zárójel
Szomorú arc (orral vagy orr nélkül)	:(vagy :-(kettőspont, (kötőjel), zárójel
Pislogás (orral vagy orr nélkül)	;) vagy ;-) kettőspont, (kötőjel), zárójel
Meglepődés (orral vagy orr nélkül)	: o vagy :-o kettőspont, (kötőjel), kis o
Nagy mosoly (orral vagy orr nélkül)	:-D vagy : D kettőspont, (kötőjel), nagy D
Kinyújtott nyelv (orral vagy orr nélkül)	: p vagy :-p kettőspont, (kötőjel), kis p

ARANYSZABÁLYOK

• Fordítsunk időt gyerekeink online kommunikációjára, és kérjük meg őket, mutassák meg, hogyan társalognak barátaikkal;

• Tanítsuk meg őket személyes adataik védelmére az interneten úgy, hogy:
- Biztonságos profilt hoznak létre a személyes beállítások alkalmazásával,
- Jelszavukat titokban tartják,
- Csak a valós életben ismert emberekkel lépnek kapcsolatba,
Csak szülői engedéllyel töltenek fel képeket magukról, a családjukról, a lakásukról, az iskoláról stb.
- Személyes információkat, mint pl. telefonszám, cím, iskola, sportcsapat stb. csak a valós életben jól ismert személyekkel osztanak meg,

• Az otthoni számítógépet a nappali jól látható részében helyezzük el, hogy figyelemmel tudjuk követni az online felhasználást.

• Együtt győződjünk meg arról, hogy tudjuk és ismerjük, hogy
- Hogyan lehet a levelezőlistáról a nem kívánt személyeket törölni,
- Az általunk használt weboldalon a biztonsági szolgáltatást aktiválni.

• Építsük fel a gyerekekkel a bizalmat úgy, hogy tévedéseikről mindig beszélhessenek velünk, hogy ezáltal a megoldásokat közösen találjuk meg! A tanuláshoz a hibázás is hozzátartozik.

HASZNOS LINKEK

Legyünk jártasak a virtuális világban és ismerjük jogainkat:
http://www.internetombudsman.hu

A Barátságos Internet Fórum segít a szülőknek az internet megértésében:
http://www.baratsagosinternet.hu

A társalgási kód feltöréséhez látogassunk el a Wikipédia honlapra és nézzünk utána az 'internetszleng' kifejezésnek:
http://hu.wikipedia.org/wiki/Internetszleng

Nézzük meg az Eurobarometer 2007. jelentését a gyerekek biztonságos internetezéséről:
http://ec.europa.eu/information_society/activities/sip/eurobarometer

3. Erőszakoskodás az interneten keresztül

EGY VIRTUÁLIS ERŐSZAKOSKODÁS ESETE

Az interneten és mobil telefonon keresztüli kommunikációnak fantasztikus előnyei vannak. Sajnos azonban kevésbé fantasztikus is lehet – gyermekeink olyan üzeneteket kaphatnak, vagy éppen küldhetnek, melyek tartalma bántó lehet számukra, vagy mások számára. Nagyon fontos, hogy megtanítsuk a gyerekeket a helyes társasági viselkedésre – nem mindig angyalok a mi gyerekeink sem ;-)

A **virtuális erőszakoskodás** során egyes emberek új információs és kommunikációs eszközöket használnak arra, hogy mást vagy másokat megsértsenek, ijesztgessenek, illetve molesztáljanak. Történhet mindez e-mailben, társalgás közben, azonnali üzenetküldésnél, mobil telefon, vagy egyéb digitális eszköz segítségével. A virtuális játék világában az erőszakoskodók megtámadhatják gyerekeink **virtuális személyiségét (avatar)**, pl. lőnek rá, ellopják virtuális javaikat vagy a virtuális személyiséget nem kívánt cselekedetekre kényszerítik.

A gyerekek gyakorta számolnak be nyilvános térben közzétett magántermészetű információkkal kapcsolatos problémákról, ilyen pl. egy magántermészetű fénykép vagy személyes adat nyilvános fórumon vagy honlapon való közzététele. Ahogy az **erőszak** az iskolában vagy a játszótéren sem elfogadott, a szülőknek, nevelőknek és a gyerekeknek egyaránt oda kell figyelniük rá, és tenniük kell ellene. A hagyományos erőszakoskodással ellentétben a virtuális erőszakoskodás akkor is érintheti a gyereket, ha az távol van az erőszakoskodótól, aki a nap bármely szakában vagy akár éjszaka is küldözgethet fenyegető üzeneteket az otthoni e-mail címre és a mobiltelefonra.

A szülők segíthetnek abban, hogy a gyerekek ne fogadják el az erőszakoskodást – tanítsuk meg őket, hogy az online névtelenség nem a felelőtlen viselkedést jelenti. Ismerniük kell saját jogaikat, felelősségüket, illetve tudniuk kell, hogyan tartsák tiszteletben mások jogait is.

Beszéljünk mindig nyíltan gyerekeinkkel, hogy bármely aggasztó probléma a felszínre kerülhessen. Az új technológiák – internet, mobiltelefon – kiváló lehetőséget nyújtanak a beszélgetésre, és gondolatébresztő hatással is bírnak!

ARANYSZABÁLYOK:

- Előzzük meg a negatív tapasztalatokat azzal, hogy meggyőződünk róla, hogy gyerekeink meg tudják védeni magánszférájukat, és tiszteletben tartják másokét is;

- Tanítsuk meg őket, hogy sértő üzenetekre ne válaszoljanak;

• Segítsünk nekik megérteni, hogy milyen üzenetek és viselkedési módok lehetnek bántóak, és hogyan lehet azokat elkerülni;

• Győződjünk meg róla, hogy ki tudják törölni a nem kívánt üzenetküldőt a kapcsolati listából;

• Mentsük el a támadó üzeneteket, szükség lehet rájuk fontos bizonyítékként;

• Ismerjük meg gyerekeink iskolai erőszakmentes stratégiáját. Szülőkkel és tanárokkal együttműködve akadályozzuk meg az erőszakosodást mind a valós, mind a virtuális életben;

• Tartsuk a kapcsolatot gyerekeink környezetével; ismerjük meg barátaikat, azok szüleit, a gyerekek tanárait, osztályfőnökét;

• Bátorítsuk gyerekeinket, hogy számoljanak be bármiféle aggasztó offline és online tapasztalatról. Legyenek biztosak abban, hogy még ha helytelenül is viselkedtek, mi mindig ott vagyunk a háttérben és segítünk közösen megtalálni a legjobb megoldást!

• Abban is legyenek biztosak a gyerekek, hogy azért soha nem ők a felelősek, ha valaki zaklatja őket.

HASZNOS LINKEK

Az alábbi honlapon olyan cikkeket találunk, melyek segítenek megismerni a virtuális erőszakoskodás problémáját:
http://www.ifiport.hu

Az internet-forródrót webes és telefonos bejelentési lehetőséget biztosít illegálisnak vagy ártalmasnak ítélet magyarországi weblapok és online tartalmak bejelentésére:
http://www.internethotline.hu

Az internet-forródrót hívószáma:

06-1-487-60-50

4. Szórakozás & Letöltés

NEM MINDEN ARANY, AMI FÉNYLIK – AZ INTERNETEN

Az internet virtuális terében számos tevékenység zajlik, többek között kereskedelem is. Ha nem vesszük meg a gyerekeinknek mindazt, amit a TV–reklámban látnak, vagy amit az üzletekben kinéznek maguknak, akkor arra is megtaníthatjuk őket, hogy azt se higgyék el és akarják megszerezni, amit online kínálnak nekik, pl. zene, játékok, **csengőhangok** és egyéb termékek vagy szolgáltatások.

Ha együtt töltjük az időt a gyerekekkel, miközben interneteznek, egyben lehetőséget kapunk arra is, hogy elmagyarázzuk nekik, hogy a különböző termékek, mint pl. csengőhangok, **háttérképek**, **mp3**, **avatar** stb. ritkán ingyenesek Ha hasonló reklámokkal találkozunk, mutassuk meg nekik az apró betűs részt, hogy megértsék, hogy nem kell mindent készpénznek venniük, amit a **neten** látnak.

Bármely szolgáltatás (ingyenes vagy fizetős) igénybevételéhez online formanyomtatványt kell kitöltenünk a megfelelő személyi adatokkal. Csak akkor töltsük ki, ha tudjuk, mire használják fel az adatainkat. Beszéljük le gyerekeinket az ilyen formanyomtatványokról, lehetőség szerint csak velünk együtt töltsenek ki ilyeneket.

A **pop-up ablak** gyakran szolgál internetes reklámfelületként. Nem mindig rosszak – attól függ, hogy megbízható honlapról származnak-e, vagy sem. Általában, ha megbízunk egy adott honlapban, a pop-up ablakban is bízhatunk. Ugyanakkor bizonyos pop-up ablakok bizonytalan termékeket reklámoznak, melyek célja egy online kérdőív kitöltése és személyes adataink megszerzése. Tanítsuk meg gyerekeinknek, hogy a pop-up ablak jobb felső sarkában lévő piros kereszttel kell bezárniuk a megbízhatatlan reklámfelületet.

ONLINE JÁTÉK

Az **online játékok** abban különböznek a régebbi digitális játékoktól, hogy **valós hálózati kapcsolatot** igényelnek. A gyerekek CD-n/DVD-n, **weboldalakon** játékkonzollal, mobiltelefonnal és egyéb hordozható eszközökkel játszhatnak.

Az online játékok között találunk egyszerűbbet, közismertet, mint pl. a Pacman és Tetris, valamint olyan virtuális valóság játékokat, ahol több játékos játszik egyszerre online és hozza létre a játék tartalmát és történetét. Sok ilyen több személyes **játék** támogatja a résztvevők virtuális közösségét. A gyerekek ez esetben ki vannak téve annak a veszélynek, hogy olyan emberekkel kerüljenek kapcsolatba az interneten, akiket nem ismernek. (ld. Kommunikáció fejezet).

A játék fontos szerepet tölt be a gyerekek fejlődésében, hiszen társas képességük és stratégiai gondolkodásuk egy fegyelmezett és szabályokat követő környezetben alakul ki. Sok vonzó és interaktív digitális játékot oktatási céllal használnak.

Persze nem minden digitális játék jó minőségű. El kell döntenünk, mely játékok a legmegfelelőbbek gyerekeink számára – és a szabályok betartásával elérhetjük, hogy a fiatalok ne más tevékenységek kárára töltsék drága idejüket online játékokkal.

A PEGI online olyan pán-európai rendszer, mely az interaktív játékokat korosztály és tartalom szerint osztályozza. A rendszert számos gyártó, pl. PlayStation, Xbox és a Nintendo, valamint Európa különböző országaiból származó kiadók és interaktív játékfejlesztők támogatják. Minden játék hátoldalán utánanézhetünk ennek a besorolásnak, - de ne feledjük, nem minden 12 éves egyforma.

FÁJLOK MEGOSZTÁSA & SZERZŐI JOG ©

A fiatalok az internetet filmek, zenék és játékok kincsesládájának tekintik, ahonnan szerintük minden letölthető, megnézhető, hallgatható és játszható. Sokszor **fájlcserélő hálózatokon** keresztül töltenek le és fel anyagokat anélkül, hogy tudatosulna bennük, hogy a **szerző** eredeti műve szerzői jogi védelem alatt áll. Ezek lehetnek filmek, dalszövegek, könyvek, szoftverek, és képek.

Ez vajon jogszerű?

A fájl megosztása nem illegális, ha olyan tartalmakat tartalmaz, melyeket mi hoztunk létre. Általában a világon mindenütt illegális, ha a szerzői jog jogosultjának engedélye nélkül töltünk fel zenét, és filmet (igaz, hogy minden egyes országnak külön szerzői joga van). Általában tekintsük a zenei és filmes fájlok megosztását illegálisnak, és legyünk óvatosak a fájlcserélő alkalmazások használatakor.

Kockázatos?

A **fájlmegosztás** során olyan kapukat (portokat) nyitunk meg a számítógépünkön, melyeken keresztül számos rosszindulatú program érkezhet a gépre, melyek akadályozhatják annak megfelelő működését. Az is elképzelhető, hogy így más is hozzáférhet személyes adatainkhoz, és a mi számítógépünket használja spamek vagy **illegális tartalmak** küldésére.

Hol találhatok jogszerűen letölthető zenét?

Világszerte honlapok százai árulnak jogszerűen zenét (ld. hasznos linkek), néha még ingyen is! Az utóbbiak általában olyan honlapok, ahol a zenészek lehetővé teszik a rajongók számára, hogy megismerjék egyes műveiket, illetve amelyeken keresztül koncertjeiket és albumjaikat reklámozzák.

ARANYSZABÁLYOK

• Győződjünk meg arról, hogy jogszerűen töltünk le zenét és filmet az internetről;

• Ösztönözzük gyerekeinket a jogtiszta tartalmú honlapok használatára, és magyarázzuk el nekik, hogy nem minden olyan amilyennek az a neten látszik;

• Magyarázzuk el az elővigyázatosság nélküli letöltések lehetséges következményeit;

• Győződjünk meg arról, hogy számítógépünk védett és naprakész anti-vírus programot tartalmaz;

• Tanítsuk meg gyerekeinket arra, hogy a szabályosan letöltött fájlokat mentsék el a merevlemezre és megnyitás előtt ellenőrizzék azokat;

• Mindig olvassuk el a titoktartási nyilatkozatot és a felhasználási feltételeket mielőtt valamit telepítünk. Ellenőrizzük (az interneten) hogy a program, amit le szeretnénk tölteni, megbízható-e;

• Zárjunk be minden bizonytalan pop-up ablakot a jobb felső sarokban lévő keresztre kattintva. Soha ne klikkeljünk az ablakra.

GYEREKEK ÉS JÁTÉKOK:

• Határozzuk meg azt az időt, amit a gyerekek játékkal tölthetnek;

• A nappaliban játszanak, ahol figyelemmel kísérhetjük őket;

• Figyeljük játékszokásaikat – ha figyelünk rájuk a játszótéren, miért ne tennénk ugyanazt virtuális közegben?

• Beszéljük meg a játék tartalmát, azt, hogy mi hasonlít a valósághoz és mi nem, mit élveznek, mit nem?

• Mielőtt megveszünk egy játékot gyerekünknek, győződjünk meg arról, hogy a tartalom a gyerek korosztályának megfelelő (pan-európai PEGI rendszer vagy egyéb nemzeti besorolás).

Ha gyerekeink több játékossal játszanak online :

• Olyan honlapot válasszunk, ahol szigorúak a szabályok és van moderátor;

- Figyelmeztessük őket, hogy személyes adataikat ne közöljék másokkal;
- Ne találkozzanak nélkülünk a többi játékossal;
- Bátorítsuk őket arra, hogy számoljanak be mindenfajta erőszakos viselkedésről, fenyegető vagy trágár stílusról, kellemetlen tartalomról, vagy játékon kívüli találkozóra szóló meghívásról;
- Vonjuk ki gyermekünket a játékból vagy változtassuk meg online azonosítóját, ha valami nincs rendben a játék körül.

HASZNOS LINKEK

Tudjunk meg többet az online játékokról és a PEGI korosztályba soroló rendszerről:
http://www.pegioline.eu

Legálisan vásárolható zenéket tartalmazó nemzetközi honlapok:
http://www.pro-music.org

A jogszerű ingyenes vagy díj ellenében hozzáférhető játékok, zenék, csengőhangok és egyéb letöltésekre vonatkozó linkeket tartalmaz a Startlap letöltésekre vonatkozó gyűjteménye:
http://www.letoltes.lap.hu

A internetes kifejezések jegyzéke magyar nyelven:
http://www.baratsagosinternet.hu

Ismerjük meg a “szakzsargont” itt:
http://www.netlingo.com

1. A Biztonság Biztonságot szül

MEGJEGYZÉSEKKEL ELLÁTOTT FELADATOK

Illesszük össze a képet a szavakkal: Számítógéház, egérpad, képernyő, hangszóró, webkamera, nyomtató, USB kártya (memóriakártya), egér, CD-Rom.

Bemelegítésképpen ismertessük meg a gyerekeket a számítógép és a hardver különböző részeivel. Ha ez megvan, mehetünk tovább.

Kérjük meg szüleinket, hogy küldjenek egy e-mailt **csatolt fájllal**, vagy küldjünk egyet mi magunknak. Gyakoroljuk a következőt: a jobb oldali gombbal a csatolt fájlra kattintva mentsük azt el a számítógép Asztalára. Az Asztalon a jobb oldali gombbal a dokumentumra kattintva ellenőrizzük azt. Ha biztosak vagyunk abban, hogy a dokumentum biztonságos, megnyithatjuk. Ne feledjük: jobb gomb és MENTÉS – ELLENŐRZÉS – MEGNYITÁS.

Küldjük egy e-mailt gyermekünk e-mail címére vagy sajátunkéra és csatoljunk egy fájlt. Kövesse gyermekünk az utasítást, mentse el a fentiek alapján, megnyitás nélkül. Miután elmentette az asztalra vagy a valamelyik mappába (pl. saját dokumentumaim), a jobb egér-gombbal a dokumentumra kattintva mégegyszer mutassuk meg neki, hogy miképpen ellenőrizze azt megnyitás előtt, hogy

rögződjön benne a biztonságos munka.

Hedvig tanácsát követve megtudhatjuk, hogyan írjuk le e-mail címünket, ha mindenképp közzé akarjuk tenni online. Ezáltal elkerülhetjük, hogy automatikusan lemásolják és visszaéljenek vele a spammerek. Példa: cybercat.smith@mymail.com = cybercat pont smith kukac mymail pont com

Gyakorlásképpen írjuk le családtagjaink e-mail címét hasonlóképpen: sajátunkat, a családi címet, apukánkét, anyukánkét.

Úgy tudjuk elkerülni az automatikus e-mail cím lemásolást és spam célokra történő felhasználását, hogy inkább betűzzük, mint hogy azt egy az egyben megadjuk. Gyakoroltassuk gyermekeinkkel a fenti gyakorlatot. Gyermekeink lehetőleg soha ne adják meg e-mail címüket az interneten, illetve olyan címet adjanak meg, amelyben a nevük nem szerepel (ld. Kommunikáció fejezet).

Hogy [s2] Zeta megérthesse mindezt, mielőtt Hedvig tovább folytatja, végezzük el az alábbi feladatokat. Karikázzuk be azokat a tevékenységeket, amelyekhez internet szükséges.

Az egészen kicsi gyerekek még nem tudhatják, mely tevékenységekhez szükséges a világháló és melyekhez nem. Egy szöveg megírásához nincs szükség internetes csatlakozásra, de a társalgáshoz már igen. A számítógépen is hallgathatunk zenét CD-ről vagy egy zenei fájlról, melyet a gépbe mentettünk el, de közvetlenül, online is hallgathatunk zenét. Csak azokat a tevékenységeket jelöljék be a gyerekek, amihez internetes kapcsolat kell.

Írjuk be szüleinkkel együtt a böngészőprogramba az alábbi címet http://kids.yahoo.com. Gyűjtsünk információkat a Tyrannosaurus Rex-ről, és próbáljuk kitalálni, mikor éltek a dinoszauruszok a Földön. Keressünk róluk képet. Ne feledjük, legalább három honlap tartalmát hasonlítsuk össze.

Tanítsuk meg gyerekeinknek, hogy ne higgyenek el mindent, amit online látnak, ezzel is helyes keresési szokásokat alakíthatunk ki. Emlékeztessük őket, hogy legalább három honlap információit összehasonlítva és felhasználva dolgozzanak, valamint a forrást mindig jelöljék meg az iskolai munkájukban.

Írjuk be szüleinkkel együtt a böngészőprogramba az alábbi címet http://kids,yahoo.com. Keressünk egy témát, például a Tyrannosaurus Rex-et, majd a három szerintünk legérdekesebb honlapot mentsük el a böngészőprogram tetején található “Kedvencek” menüre kattintva. Létrehozhatod saját mappádat is.

Érdekes honlapok elmentése és azok rendezése a Kedvencek mappában (a böngészőprogram eszköztárában található) jó lehetőség arra, hogy a kis gyerekeknek ne kelljen mindig az interneten keresgélniük az információt.

SIKERÜLT MEGÉRTENI?

1: (biztonságos) 2: (vírus),(ismeretlen), (letöltés), (fertőzött),(memóriakártya), (nem védett) 3: (furcsán) 4: (ismeretlen),(csatolmány), (ígérnek), (spam) 5: (egyetlen egy), (spam) 6: (első), (három),(összehasonlítás),(bárki), (közzététel) 7: (anti-vírus), (anti-kémszoftver) 8: (beszél), (szülők) 9: (mond)

JAVASOLT MEGOLDÁSOK A SZITUÁCIÓS KÁRTYÁKHOZ

SZITUÁCIÓ 1. Soha ne szörföljünk az interneten, ha számítógépünkön nincs naprakész anti-vírus és anti-kémszoftver program. Olyan ez, mint határ határőrök nélkül; káros programok támadhatják meg a gépet, olyanok, mint: vírusok, trójai lovak, férgek vagy kémszoftverek.

SZITUÁCIÓ 2. Legyünk óvatosak az ismeretlenektől kapott e-mailekkel szemben, főleg ha csatolt fájlt tartalmaznak, illetve ha sokat ígérő, csábító az üzenet – ezek leggyakrabban spamek! Olyan káros programokkal fertőzhetik meg a spamek a gépet, mint pl. vírusok, trójai lovak, férgek vagy kémszoftverek. Ne nyissuk meg ezeket a leveleket. Helyette az e-mailre kattintva a jobb oldali gombbal zárhatjuk ki a feladót (‘Block sender’) vagy egyszerűen csak töröljük az e-mailt.

SZITUÁCIÓ 3. Ha információt keresünk az interneten, ne bízzunk azonnal az első honlapban. Legalább három honlap tartalmát hasonlítsuk össze. Ne feledjük: akinek internet-csatlakozása van, az létre tud hozni információt a neten. Ha egy jelentést, vagy egy dolgozatot írunk, mindig jelezzük a forrást, és a képet, ahonnan másoltuk. ...ezt tenné egy igazi kutató is.

2. Kommunikáció ;-D

MEGJEGYZÉSEKKEL ELLÁTOTT FELADATOK

Jelöljük meg, hogy számunkra mi mennyire **magánjellegű** információ: telefonszámom, hajszín, nevem, az ország, ahol élek, iskolám, lakcímem, állatom neve, szüleim foglalkozása, e-mail címem, fényképem, korom.

Gyermekünk számára vajon a magánügy ugyanazt jelenti, mint az Ön számára? Három színt használva megtudhatjuk: nagyon magánügy (piros), eléggé magánügy (narancssárga), nem magánügy (zöld).

Segítsünk Zetának az igazán jó jelszó kitalálásában Hedvig ötletei alapján:

A jó jelszó különböző adatokból áll (számok, betűk, írásjelek) és mindig titokban kell tartani.

Kövessük Zeta példáját és hozzunk létre egy biztonságos profilt, majd egy nem biztonságosat is:

Hozzanak létre a gyerekek egy biztonságos, majd egy nem biztonságos profilt, mely személyes adatokat tartalmaz. Arra azért figyelmeztessük őket, hogy hiába hoznak létre biztonságos profilt, ha később adataikat online közzé teszik.

Nézzük meg ezt a képet, és mondjuk el, mi a véleményünk az illetőről:

Milyen személyes információkra tudunk következtetni a képből? A gyerekek sokszor nem ismerik a kép hatalmát.

‘Zeta ötletét követve gondoljunk ki 3 dolgot, amit Alex, mint Piroska, Hedvigtől kapna, hogy megvédje magát a “web-farkasoktól”.

Ellenőrizzük, hogy a gyerekek megértették-e az idegenekkel való kapcsolatfelvétel veszélyeit.

Mit szeretnél, hogyan bánjanak veled az emberek az interneten? (1..... 2..... 3.....)

Győződjünk meg arról, hogy a gyerekek megértették, hogy nekik is úgy kell viselkedniük online, ahogy ők szeretnék, hogy velük viselkedjenek....

A KÓD MEGFEJTÉSE: fedezzük fel, mit jelenthetnek a legnépszerűbb chat betűszavak:

A betűszavak/mozaikszavak megértésében segít a Kommunikáció - Netikett, chat nyelv fejezet.

A billentyűzet segítségével létrehozhatjuk az emotikonokat: a mosolygós –szomorú arcot - pislogót - meglepődöttet –nagy mosollyal – kinyújtott nyelvvel

Bővebben a Kommunikáció -Netikett, chat nyelv fejezetben olvashatnak erről.

SIKERÜLT MEGÉRTENI?

1: (profil) 2: (személyes adat védelme), (felelős) 3: (idegenek),(mond) 4:(Netikett),(kezel) 5: (emotikon) 6: (jelszó), (írásjel) 7: (titok) 8: (nem továbbít) 9: (ismerős)

JAVASOLT MEGOLDÁSOK A SZITUÁCIÓS KÁRTYÁKHOZ

SZITUÁCIÓ 4. Ha internetezünk vagy a profilunkat használjuk és adatokat adunk meg magunkról, azokat emberek százai, ezrei, sőt milliói is olvashatják. Ezért fontos alaposan megválogatni a magunkról megadott információkat. Csak olyan embereknek adjuk meg személyes adatainkat, akiket a valós életben is jól ismerünk, és akikben megbízunk.

SZITUÁCIÓ 5. Mike minden bizonnyal elárulta jelszavát barátjának, aki ezzel visszaélve trágár e-maileket küldözget a nevében. Mindig tartsuk titokban jelszavunkat, hacsak nem akarjuk, hogy más is elolvassa leveleinket és a mi nevünkben olyanokat írjon, amik nekünk eszünkbe sem jutnának!

SZITUÁCIÓ 6. Az idegennel való találkozás nem túl jó ötlet. Ha azonban úgy gondoljuk, hogy megbízhatunk online barátunkban, aki szeretne találkozni velünk, mondjuk el szüleinknek, hogy valaki elkísérhessen. Őszinte barátnál ez nem probléma. Csak olyan embereknek jelent gondot, akik valamit eltitkolnak.

3. Erőszakoskodás az interneten keresztül

MEGJEGYZÉSEKKEL ELLÁTOTT FELADATOK

Rajzoljuk le milyen meghívót kapott Alex tanáraitól. Mutassuk meg milyen erőszakmentes logót és szlogent használ az iskola az erőszakmentes hét alkalmából.

Hagyjuk, hogy kreatívan tudjanak kibontakozni a gyerekek, és rajzoljanak az üres keretbe.

Alex példáját követve találjunk öt okot, ami miatt "piros lapot" adhatnánk valakinek.

Beszéljük meg gyerekeinkkel, milyen viselkedést tartanak elfogadhatatlannak.

SIKERÜLT MEGÉRTENI?

1: (szabályszerű), (elront) 2: (megbeszél) 3: (jó) 4: (virtuális erőszakoskodás) 5: (visszautasít/blokkol) 6: (ismerős) 7: (válasz)

JAVASOLT MEGOLDÁSOK A SZITUÁCIÓS KÁRTYÁKHOZ

SZITUÁCIÓ 7. Ez semmi esetre sem megfelelő módja a mobiltelefon használatának. Ne küldözgessünk olyan üzeneteket, képeket, vagy egyéb anyagokat, melyek károsak lehetnek. Bánjunk úgy másokkal, ahogy mi szeretnénk, hogy velünk bánjanak. Ilyen esetekben beszéljünk szüleinkkel vagy egy olyan felnőttel, akiben megbízunk.

SZITUÁCIÓ 8. Alexnak el kellene mondania barátjának, hogy az erőszakoskodó személy magatartásáról nem ő tehet. Nem kellene az üzenetre válaszolnia, de meg kellene őriznie bizonyítékként és megmutatni szüleinek vagy tanárainak. Alexnak szüleivel is beszélnie kellene az esetről, akik támogathatják abban, hogy barátjának segítsen.

SZITUÁCIÓ 9 Netiquette az, amikor úgy bánunk emberekkel a neten, ahogy mi szeretnénk, hogy velünk bánjanak. Mostanra már biztos eleget tudsz ahhoz, hogy segíts Zetának a feladatban.

4. Szórakozás & Letöltés

MEGJEGYZÉSEKKEL ELLÁTOTT FELADATOK

Nyissuk meg kedvenc keresőprogramunkat. Írjuk be azt, hogy “ingyenes csengőhangok” vagy azt, hogy “ingyenes játékok”, és nézzük meg, mi történik. Ellenőrizzünk néhány honlapot. Megtaláltuk a csapdát?

Adott jelszavakkal gyakoroljuk a keresést és nézzük meg a honlapokat, hogy mi a csapda. Vegyük észre az apró betűs részt is, amit szépen kihagynak a reklámoldal szlogenjéből.

Mi a kedvenc számítógépes játékod? Ellenőrizzük, hogy szüleink ismerik-e, és ha igen hogyan? Ha fogalmuk sincs róla, meséljük el nekik, majd hagyjuk, hogy röviden leírják a játékot. Sikerült nekik? Tízből hány pontot adnánk nekik? .../10
A szülő összefoglalja gyermeke kedvenc játékát, aki rajzol róla egy képet.

Valóban tudjuk, milyen játékokat játszanak gyerekeink online és azt is, melyek a kedvenceik? Hagyjuk, ellenőrizzék csak le!

SIKERÜLT MEGÉRTENI?

1: (ingyenes) 2: (formanyomtatvány) 3: (csapdák) 4: (illegális) 5: (kereszt) 6: (figyelmen kívül hagy) 7: (magánügy) 8: (megoszt), (te magad) 9: (letölt)

JAVASOLT MEGOLDÁSOK A SZITUÁCIÓS KÁRTYÁKHOZ

SZITUÁCIÓ 10. Az interneten található legtöbb zene és film illegális másolat. Ráadásul azok a honlapok, melyeken zenék és filmek cserélnek gazdát, általában tele vannak olyan káros programokkal, mint amilyenek pl. a trójai ló, a férgek, illetve a kémszoftverek. A helyes megoldás, amit Zetának választani kellene, a “b” vagy a “c”. Természetesen kedvenc jogtiszta zenéjének letöltése egy közkedvelt honlapról kevesebbe kerül, mint egy teljes CD megvásárlása. Szülei véleményét és engedélyét kellene kikérnie.

SZITUÁCIÓ 11. Számos ingyenes szolgáltatás található az interneten, de a csengőhangok, háttérképek, MP3, avatar és hasonlók ritkán tartoznak közéjük. Ha Alex figyelmesebben megnézi a honlapot, biztos észreveszi az apró betűs részt is, amely elmagyarázza a szolgáltatás valós árát. Csengőhangok, kvízek, játékok stb., kiváló lehetőség emberek becsapására, hogy ún. "ingyenes" szolgáltatásokra iratkozzanak fel, ami valójában pénzbe fog kerülni.

SZITUÁCIÓ 12. Alexnak nem szabadna elfelejtenie, hogy személyes adatai nem nyilvánosak, ha online játszik olyanokkal, akiket nem is ismer valójában. Nem kell megadnia, hol lakik, iskolája adatait, vezetéknevét stb. Szüleit tájékoztatnia kellene a játékairól, és soha nem szabad letöltenie játékot az internetről szülői engedély nélkül, mivel az károsíthatja az otthoni számítógépet.

D. Szószedet

Anti-kémszoftver: olyan program, mely a kémszoftverek ellen harcol. Minden beérkező adatot átvizsgál és kiszűri a káros elemeket, amiket talál vagy listát készít, amelyről a gyanús programokat ki lehet törölni.

Anti-vírus: számítógépes program, mely azonosítja, elkülöníti, feltartóztatja, eltávolítja a vírusokat és az egyéb rosszindulatú szoftvereket a gépből. Az anti-vírus általában átvizsgálja a fájlokat, megkeresi az ismert vírusokat, majd azonosítja a számítógépes programok gyanús viselkedését, melyek fertőzöttek lehetnek.

Avatar: a felhasználó profilja, névvel és képpel, ikonnal vagy egy 3D-s karakterrel ellátva, melyeket általában online számítógépes játékoknál és a virtuális világban használunk.

Azonnali Üzenetküldő Szolgáltatás: azonnali és szimultán elektronikus kommunikáció két vagy több felhasználó között. A szolgáltatás lehetővé teszi, hogy meghatározott személyekkel társalogjunk. Ha címlistánkról valaki online tartózkodik, erről azonnal értesítést kapunk.

Azonosító: az azonosító, a felhasználói név és a jelszó engedélyével hitelesen vehetünk igénybe online szolgáltatásokat. Operációs rendszerünk segítségével minden családtag számára különböző azonosítót hozhatunk létre.

Becenév: a képernyőnév szinonímája. Az online szolgáltatás felhasználója maga hozza létre a becenevét. A címlista, chat szoba stb. felhasználójának is van beceneve. Ha jól választjuk meg a becenevet, megőrizhetjük névtelenségünket online.

Betűszó: olyan rövidítés, mely egy kifejezés vagy mondat szavainak első betűiből áll. Általában a társalgás során használják a kommunikáció gyorsítására. Angol példák: LoL, (Laughing Out Loud/Lots of Laugh) CU, Btw (ld. Kommunikáció fejezet).

Biztonsági beállítás (profil): személyre szabott biztonsági lehetőség az online profilhoz kapcsolva (ld. definíció). Általában képek és fájlok megnyitásánál fontos, hogy beazonosítsa a megbízható információ küldőjét és engedélyezze a felnőtteknek vagy a gyerekeknek szóló tartalmat.

Blog: a weblog rövidítése. Olyan honlap, mely tartalmát egyének vagy csoportok írják, általában naponta, képekkel, audiovizuális fájlokkal, és linkekkel.

Blogging: a blog aktualizálása, írása.

Böngészés: a böngésző használata honlapok megtekintésére, vagy az interneten történő szörfölés.

Böngésző: honlapok megtekintésére szolgáló program. A Windows leggyakoribb böngészői az Internet Explorer, a Netscape Navigator és a Firefox, míg a Safari a Machintos böngésző programja. A korszerűbb böngészők innovatív szülői ellenőrzésre is lehetőséget nyújtanak.

CD-Rom: a „Compact Disc csak olvasható memóriával" angol kifejezés betűszava. Olyan Compact Disc, amelyre nem lehet semmit felvenni, és amely csak számítógép által olvasható. A CD-ROM-okat általában számítógépes szoftverek terjesztéséhez használják.

Címlista: online játékok, mobiltelefonok e-mailek és azonnali üzenetküldő stb. szolgáltatások listája, a lista bővíthető, elutasítható és kitörölhető.

Computer fájl: a számítógépben, adott fájlnévvel elmentett adott információk archívuma/gyűjteménye (dokumentumok, programok stb.). Az irodai vagy könyvtári papírdokumentumok modern változatainak is tekinthetők.

Computer program: általában szoftverként említjük. A szoftver strukturált utasításokat tartalmaz, melyeket programozók írnak, ez alapján működik a számítógép. Általában CD-Rom-on veszünk szoftvert (ld. definíció), mely az adathordozók kézzel fogható megjelenítése.

Családi beállítás: szülői felügyelet más néven. Egyedi igényeknek megfelelően be lehet állítani a böngészőt vagy más web eszközt, hogy az gyerekbarát módon működjön, tehát legyen benne tartalomszűrő, időkorlátozó, játékszabályozó stb.

Csatolmány: olyan számítógépes fájl, melyet e-maillel együtt lehet küldeni. A férgek és a vírusok általában csatolt fájllal terjednek. Az ismeretlenektől érkező, csatolmányt tartalmazó fájlokat mindig gyanúsnak kell tekinteni.

Csengőhang: a beérkező hívást jelző mobiltelefon-csengés. Széles a választék a gyakorta díjfizetés ellenében személyre szabható és letölthető hangokból és zenéből.

Digitális játék: játékfejlesztők által létrehozott számítógépes játék. Az online játékok olyan digitá-

lis játékok, melyhez élő hálózati kapcsolat szükséges. Ezeket egyszerre több játékos is játszhatja.

Előfizetés/Feliratkozás: szolgáltatásra, vagy naprakész hírekre történő önkéntes regisztráció, ezáltal az információ közvetlenül a személyes levelezőládánkba érkezik.

E-mail: elektronikus írott kommunikációs eszköz. Üzenetek küldésére alkalmas bármilyen fájllal együtt – szöveg, kép, hang és egyéb.

E-mail cím: virtuális hely, ahova az e-mail üzenetek érkeznek. Az e-mail címek két részből állnak, amelyeket a @ jel választ el.

Emotikon: olyan kép vagy ikon, mely érzelmeket fejez ki, pl. mosolygós arc. A billentyűzeten lévő írásjelek segítségével hozhatjuk létre. A társalgási és játék szobákban, valamint az azonnali üzenetküldő szolgáltatásnál és a mobiltelefonokon stb. kész jeleket is találunk.

Erőszakoskodás: ismétlődő zaklatás, fenyegetés, sértegetés, akár szexuális megjegyzésekkel, fizikai támadásokkal, vagy becsmérlő beszédekkel.

Eszköztár: ikonok és jelzések együttese, a szoftver program része. Mindig elérhető, könnyen használható, a mindennapi munkák és feladatok ellátását segíti.

Fájl megosztás: a felhasználók közötti online fájl-csere. Fájlok küldése mások számára (feltöltés) és internetről történő lemásolása a gépre (letöltés). Általában egyenrangú hálózatban történik (P2P: peer-to-peer).

Fájltovábbítás: a számítógépes hálózaton keresztül lehet a fájlokat továbbítani. A felhasználók szemszögéből ez vagy feltöltést, vagy letöltést jelent.

Felhasználói profil: információk gyűjteménye, a szoftver, a weboldal vagy egyéb technikai eszköz felhasználóját jellemzi. Olyan információkat tartalmaz, mint a felhasználónév, a jelszó és egyéb adatok (pl. születési dátum, érdeklődés).

Feliratkozás: online szolgáltatásra történő feliratkozás: újság, vitafórum, e-mail, társalgás stb. Normális esetben a felhasználók eldönthetik, mikor szeretnének leiratkozni.

Feltörés: kereskedelmi szoftverek illegális másolása a szerzői jog megsértésével.

Féreg: speciális önsokszorosító vírus, mely a számítógép használójának tudta nélkül terjed gépről gépre, károsítja a hálózatot, rendkívüli méretű sávszélességet foglal, kikapcsolja a számítógépet stb.

Flaming/Indulatkitörés: ellenséges, bántó viselkedés az internet felhasználók között. Rendszerint vitaoldalakon, Internet Relay Chat-ben (IRC) vagy e-mailben fordul elő.

Formanyomtatvány (online): formázott dokumentum táblázatokkal, melyeket adatainkkal kell kitölteni. Az elektronikus formanyomtatványt szabadon vagy előre megadott válasz-

lehetőségekkel kell kitölteni (legördülő menü). Elküldése után megtörténik az adatfeldolgozás, mely során közvetlenül az adatbázisba kerülnek az adatok.

Forródrót: telefonvonal vagy web-alapú szogáltatás, ahol az illegális tartalmakkal vagy az internettel kapcsolatban panaszt lehet tenni. Mindenki számára elérhető hatékony szolgáltatás, melyet az adott ország kormánya, ipari testületei, és internet-felhasználói támogatnak.

Fórum: online, közös érdeklődésű társalgási csoport, ahol a résztvevők különböző témákban nyíltan váltanak üzenetet.

Főoldal/Honlap: az a weboldal, mely automatikusan megjelenik a böngészőben. A kifejezés az első oldalra, vagy a honlap fő oldalára utal (ld. definíció).

Grooming: pedofilok által használt online társalgási szoba, akik elhitetik a gyerekekkel, hogy diáktársaik. Beszélgetéseket kezdeményeznek úgy, hogy közben az áldozatokról információkat gyűjtenek pl. lakóhely, érdeklődés, hobby, szexuális tapasztalatok. Számos eszközük van a gyerekek szexuális témájú társalgásba való bevonására.

Gyermekpornográfia: a gyermekpornográfiának minden országban eltérő definíciója van. Általában olyan képet jelent, amely egy gyereket kifejezetten szexuális tevékenység közben ábrázol.

Hacker/számítógépes kódtörő: leggyakrabban olyan személyekre használják, akik számítógépes kódokat törnek fel (ld. 'cracker'). Informatikai körökben számítógép rajongó is lehet.

Hardver: a számítógép kézzel fogható része, megkülönböztetve a szoftvertől, mely a hardveren működik. Belső tartozékok: nyomtatott áramköri lapok (motherboards), merevlemez, és RAM – ezeket gyakran alkotórészeknek hívjuk; illetve a külső tartozékok: képernyő, billentyűzet, nyomtató stb. – ezeket a gép perifériaegységeinek is hívjuk.

Háttérkép: a képernyő háttereként szolgáló kép, vagy egyéb grafikai ábrázolás.

Hírcsoport: ld. Fórum definíciója.

Illegális tartalom: nemzeti szabályokba ütköző jogellenes tartalom. Leggyakrabbak a gyerekekről készült szexuális képek, chat szobákban végzett jogellenes tevékenységek (pl. grooming), online gyűlöletkeltés és idegengyűlölettel kapcsolatos honlapok.

Internet: világméretű, nyilvánosan hozzáférhető számítógépes hálózat, melyen keresztül adatcsere és -átvitel zajlik. Helyi, tudományos, üzleti és kormányzati hálózatok léteznek különböző szolgáltatásokkal, mint pl. e-mail, online társalgás, információ továbbítás stb.
Internet kapcsolat: arra utal, amikor a felhasználó az internetre kapcsolódik. Internet kapcsolat általában tárcsázással, T-line-on, Wi-Fi-n, műholdon illetve mobiltelefonon keresztül jön létre.

IP-hálózaton keresztül történő beszédátvitel (VoIP): olyan technológia, mely a szoftver letöltése után lehetővé teszi az interneten keresztüli beszélgetést. A hívások ingyenesek lehetnek, ha a felhasználók ugyanazon a VoIP rendszeren hívják egymást (pl. Skype, Voicebuster). Az ilyen

szoftverek általában társalgási és fájlmegosztási lehetőségeket is tartalmaznak.

Jelentés: nyilvános virtuális helyek felhasználóinak lehetőségük van problémák jelentésére (technikai, elfogadhatatlan felhasználói viselkedés, illegális tartalom, stb.) a moderátor felé.

Jelszó: betűk titkos csoportja, melynek segítségével a felhasználó hozzáférhet fájlokhoz, a géphez, illetve programokhoz. Biztonsági eszköz az engedély nélküli felhasználók ellen (ld. Kommunikáció fejezet).

Káros tartalom: kép, szöveg, dokumentum stb., melynek tartalma ártalmas lehet, pl. az erőszakot ábrázoló képek károsak lehetnek a gyerekekre és a fiatalokra.

Kedvencek: egyedi igényekre szabott mappa, ahol kedvenc linkjeinket/könyvjelzőnket tárolhatjuk. A kedvencek aztán al-mappába sorolhatók és/vagy azokat kulcsszavakkal nevezhetjük el a keresés egyszerűsítésére.

Kereső: eszköz, mely a honlapon adott információkat keres. A legismertebbek: Google és MSN kereső. Felhasználói preferenciákat tartalmaz, melyek között érdekes biztonsági beállítások találhatók.

Kémszoftver: rosszindulatú szoftver, melyet titkosan csatoltak az internetről letöltött fájlhoz, feltölti magát a személyi számítógépre és figyeli a gépen végzett műveleteket. Az információt harmadik személynek, gyakran olyan vállalatoknak küldi el, akik személyes profiljainkra kíváncsiak, melyek alapján reklámokat vagy egyéb információkat küldhetnek számunkra, vagy olyan számítógépes kalózoknak, akik személyes adatainkhoz szeretnének hozzáférni..

Képernyőnév: ld. becenév definícióját.

Kísérleti szoftver: olyan szoftver, melyet megvásárlás előtt ki lehet próbálni. A kísérleti verzió általában mindent tud, amit az eredeti szoftver, azzal a különbséggel, hogy korlátozott időre szól.

Könyvtár: rendszerező program, mely a számítógépben hierarchikusan rendezi el a mappákat, és fájlokat. Pl. Dokumentumaim, Képeim, stb.

Közösségi hálózat: hasonló érdeklődésű online közösségi tagok, akik online teremtenek kapcsolatot egymással a megfelelő szoftver és szolgáltatás segítségével (ld. virtuális közösségi hálózat).

Közösségi kapcsolatépítő honlapok: olyan virtuális terek, melyek a közösség azonos érdekeltségű tagjait fogadják. A tagoknak felhasználói profillal kell rendelkezniük és megoszthatnak eszközöket szövegek, képek, egyéb fájlok feltöltésével, üzeneteket továbbíthatnak és fórumokon vehetnek részt. Sok olyan közösségi kapcsolatépítő honlap létezik, amely a 13 év alatti gyerekek számára tilos, ezek biztonsági profil-beállítással vannak ellátva.

Letölt: online szolgáltatásról történő fájl másolása a számítógépbe.

Limlom mail: akaratlanul fogadott, majdnem egyező e-mail üzenetek, amelyek a felhasználók e-mail címére érkeznek. Mivel az internet nyilvános, kevés esélye van annak, hogy elkerüljük a limlom leveleket, mint ahogy a spameket is nehéz kiküszöbölni.

Link: Online dokumentumra való hivatkozás (honlap, szöveg, kép stb.). Ha a linkre kattintunk, új oldal jelenik meg, vagy egy teljesen más honlap. A szöveges linkek általában kékek és alá vannak húzva, de lehetnek ettől eltérőek is. A képek is lehetnek linkek, melyek más honlapokra vezetnek el.

Magánügy: olyan személyre vagy csoportra vonatkozó dolgok, melyek nem tartoznak a nyilvánosságra. Valaki magánügye sokszor vele járóan speciális vagy érzékeny terület.

Malware: a károkozó szoftver rövidítése, mely a számítógépes rendszer tönkretételét célozza meg a tulajdonos tudta nélkül. Számítógépes vírusokat, férgeket, trójai lovakat, kémszoftvereket és egyéb rosszindulatú nem kívánt szoftvereket tartalmaz.

Manipulálás: egy kép, fájl, fotó vagy illusztráció megváltoztatása látható vagy láthatatlan módon. Napjainkban számos eszköz áll rendelkezésre a tartalmak befolyásolására, adatok finomítására, melyek eredménye eltér a valóságtól.

Mappa: fájlrendszeren belüli fájlcsoport és/vagy egyéb könyvtár. Az információk rendszerezésére szolgál, és különböző dokumentumokat tartalmaz.

Second Life: a Linden Labs amerikai cég jól ismert 3D virtuális közössége. Az avatar (ld. definíció) segítségével virtuálisan játszhatnak a játékosok, létrehozhatnak otthonokat, különböző környezeti elemeket, kereskedhetnek, és pl. virtuális pénzt is kereshetnek.

Memóriakártya/USB/: adattároló USB csatlakozóval (univerzális). Általában kicsi, könnyű, kivehető és újraírható.

Mobil: elektronikus telekommunikációs eszköz, azaz mobiltelefon, gsm, intelligens telefon. Alapjaiban ugyanazt a szolgáltatást nyújtja, mint a hagyományos vonalas telefon. Ma a legtöbb mobilban kamera is található, és internetes csatlakozásra is alkalmasak (fizetős szolgáltatás).

Mp3: audio-specifikus kódolt lejátszó. Ami a méretet illeti, egy mp3 fájl az eredeti audiofájl tizede, de a hangja megközelíti a CD minőséget. Kis mérete és minősége miatt az mp3 a zenetárolás kedvelt eszköze lett mind a számítógépen, mind pedig mobil eszközökön.

Net: az internet rövidítése.

Netikett: internetes etikett, mely az online kommunikáció udvariassági szabályait határozza meg.

Operációs rendszer: a számítógép alapfunkcióit működteti, amelyek segítségével a többi program is működik. Ismert példák a Windows, a Linux és a Mac OS.

Pop-up ablak: egy honlap megnyitása, vagy egy speciális gomb megnyomása során hirtelen fel-

bukkanó ablak. A pop-up ablakok általában parancsmenüt tartalmaznak és addig a képernyőn maradnak, amíg ki nem választjuk az adott menüt vagy be nem zárjuk a jobb felső sarkában lévő piros keresztre kattintva.

Port: interfész a számítógépen, mellyel egy másik készülékhez lehet csatlakozni. A port lehet belső vagy külső is. A belső port lemezmeghajtóhoz vagy hálózathoz kapcsolódik, míg a külső port a gép periférikus részeihez csatlakozik, mint pl. nyomtató vagy billentyűzet.

Processzor: vagy Központi Feldolgozó Egység (CPU) a számítógép része, mely adatokat dolgoz fel, jelzőberendezéseket hoz létre és tárolja az eredményeket. A számítógép memóriájával együtt, a gép központi részét képezi.

Profil: személyes felhasználói információ a közösségi hálózatoknál, azonnali üzenetküldésnél, online társalgásnál, online játéknál stb. Lehet nyilvános és privát, a felhasználó határozza meg, hiszen virtuális helyeken őt jeleníti meg.

Programfeltörő: informatikai rendszerbe illegálisan betörő személy.

P2P hálózat: a peer-to-peer (P2P) hálózatban lévők számára lehetséges a fájlcsere feltöltéssel és letöltéssel (ld. definíció). Ez az interneten lehetséges fájlmegosztások egyik módja. Néhány fájlmegosztási szolgáltatás jogellenes.

Riasztás: figyelmeztető jelzés a képernyőn, mely akkor jelenik meg, ha potenciális veszélyben van a program és a gép. Pl. új levél, a játék állása, vagy anti-vírus védelem.

Segélyvonal: e-mail vagy néha telefonszolgáltatás, melyet számos országban gyermeksegítő szervezetek és Insafe hálózatok tagjai támogatnak. A gyerekek az online technológia során az őket ért illegális vagy káros tartalmakról, kellemetlen és ijesztő élményeikről számolhatnak be.

SIP-Bench: az Európai Bizottság által támogatott tanulmány, melyben 30 felügyeleti és anti-spam eszközt teszteltek, hogy azok mennyire hatékonyak a gyermekeket sértő káros internetes tartalmakkal szemben.

Sok résztvevős online játék: 3 dimenziós népszerű játékok játékosok ezreivel, akik fiktív szerepeket töltenek be és egymással versenyeznek. A szerepjátékok is ilyenek, ahol a résztvevők együttműködve, saját maguk hozzák létre a történetet.

Spam: nem kívánt, ömlesztett e-mailek, általában kereskedelmi céllal. A spamküldés a leghírhedtebb internetes háborgatás.

Spam szűrő: kizárja a spam üzeneteket, ezáltal nem menti el azokat a gép a beérkezett üzenetek közé.

Sütik: internetes honlapok által a számítógépünkön hagyott kicsi adatcsomagok. Minden alkalommal, amikor megnyitjuk a honlapot, a süti jelez annak a szervernek, amelyen a honlap található. A sütik mutatják, hogy milyen honlapokat kedvelünk, és azok az online vásárlásnál is használatosak. A sütik elutasítása használhatatlanná tehet bizonyos honlapokat.

Szabad és részben szabad szoftver: általában szerzői jog védi a szoftvereket, ezért nem lehet letölteni őket. A szabad szoftver azt jelenti, hogy szerzője belegyezik annak ingyenes használatába. A részben szabad szoftver azt jelenti, hogy a szerzője próbaidőre engedélyezi annak bárki általi felhasználását, melynek lejárta után fizetni kell a további használatért.

Személyes adatok: bármely információ, mely egy személyhez kötődik. A személyes adatok gyűjtésének, feldolgozásának és tárolásának célját pontosan meg kell határozni.

Személyes beállítások: azonosító-specifikus személyes adatokat szerkeszthetünk annak érdekében, hogy megakadályozzuk a személyes információk, sütik stb. közzétételét.

Személyiség lopás: személyes adatok lopása (pl. név, születési dátum, hitelkártya száma) és azok illegális használata.

Szemét/Limlom/Spam mappa: az e-mail levélszekrény azon része, ahol a szemétnek nyilvánított levelek vannak.

Szerző: irodalmi vagy audiovizuális mű, szoftver stb. szerzője. A szerzői jog a szerzők alkotásait védi az illegális másolásoktól.

Szerzői jog: kizárólagos jogosultság, mely egy ötlet, mű, vagy információ felhasználását szabályozza. A szerzői jogot ez a jel szimbolizálja "©".

Szkennelés: nyomtatott anyag digitalizálásának folyamata szkenner felhasználásával. A konvertálás lehetővé teszi az adott dokumentum elektronikus formában történő tárolását és online továbbítását.

Szoftver: ld. a számítógépes program definícióját.

Szülői felügyelet: ld. Családi beállítás definícióját.

Szűrő: az információk elérését vagy speciális internetes szolgáltatást szabályozó eszköz, mely figyelmeztet ha problémás honlapot talál, követi a felhasználó útvonalát, lezárja a kockázatos oldalakat sőt a gépet is kikapcsolja veszély esetén. Szűrőrendszereket többek között számítógépekre, szerverekre, internetes telefonokra lehet telepíteni.

Társalgás (Chat): írott, egyidejű kommunikáció az interneten keresztül, chat és azonnali üzenetküldő alkalmazás segítségével (pl. MSN).

Társalgó szoba (Chat room): nyilvános virtuális hely valós időben történő kommunikációra. A világ minden részéről találkozhatnak itt egymással az emberek és üzeneteiken keresztül a billentyűzet segítségével beszélgethetnek. Ha gyerekeink társalognak, ügyeljünk arra, hogy korosztályuknak megfelelően tegyék, moderátorral és felügyelettel.

Titoktartás: egy személy vagy csoport arra irányuló képessége, hogy ellenőrizze a rá vonatkozó információ áramlását, és ezáltal akaratától függően jelenjen meg. A titok esetenként a névtelenséghez kapcsolódik, vagyis ahhoz a törekvéshez, hogy a nyilvánosság számára a felhasználó

láthatatlan maradjon.

Trójai lovak: rosszindulatú kód, szoftver, mely problémamentesnek tűnő tevékenységekkel, mint pl. játékokkal, vagy éppen víruskereső programokkal lopakodik be a számítógépbe. A Trójai lovak ugyan nem sokszorozzák meg magukat, de céljuk ugyanúgy a titkos és személyes információk megszerzése vagy tönkretétele. Kitörölhetik a merevlemez tartalmát is.

Tűzfal: hardver (útvonalválasztóba integrálva) vagy szoftver (a személyi számítógépben), mely az engedély nélküli felhasználókat (pl. hackers és crackers) megakadályozza abban, hogy az internetre csatlakoztatott számítógéphez, annak hálózatához hozzáférjenek.

URL (Uniform Resource Locator): egy adott weboldal vagy fájl címe az interneten. Nem tartalmaz speciális betűket vagy szóközöket. A perjelek jelzik a különböző könyvtárakat. A cím első része a protokollt jelzi, a második az IP címet vagy a tartománynevet, ahol a forrás található.

Újra hasznosító kuka: számítógépes katalógus, ahol a kitörölt fájlok ideiglenesen tárolva vannak, mielőtt a felhasználó végleg kitörli azokat. Rendszeresen el kell távolítani a kukából a régi és szükségtelen adatokat, hogy helyet szabadítsunk fel a merevlemezen, a gép belsejében.

Virtuális erőszakoskodás: az elektronikus médián keresztüli erőszakoskodás, általában azonnali üzenetküldés vagy e-mailezés során, ismétlődő sértegetés, megfenyítés, szexuális zaklatás és becsmérlő beszéd formájában. A virtuális erőszakoskodó nyilvánosságra hozhatja az áldozat személyes adatait, illetve nevében információkat közölhet, hogy az illetőt nevetségessé tegye vagy rágalmazza.

Virtuális javak: olyan tárgyak, melyeket a játék résztvevői birtokolnak. Minden játékos birtokolhatja ezeket a tárgyakat, amit a számítógép terminálja jelez.

Vírus: olyan rosszindulatú kód, szoftver, mely felhasználói beavatkozással terjed. Általában e-mail csatolmányok, vagy fertőzött külső memóriaeszközök (USB, CD-Rom) útján terjed.

Web: a World Wide Web/világháló rövidítése. HTML (HyperText Markup Language) formátumú online dokumentumok gyűjteménye, melyek linkeket tartalmaznak más dokumentumokhoz pl. grafikákhoz, audio és videó fájlokhoz. A web az internet egy része.

Webkamera: olyan kamera, mely a weben keresztül működik azonnali üzenetküldő, PC videó konferencia, társalgás stb. lehetőségek során. A webkamera olyan digitális kamera, mely a web szerverére folyamatosan vagy időközönként tölti fel a képeket.

Weboldal: a világháló egyik helye, oldala. Minden weboldal tartalmaz honlapot, mely az első dokumentum, amikor megnyitjuk az oldalt. A weboldalak általában további fájlokhoz, honlapokhoz vezetnek el linkek segítségével. A weboldalak magánszemélyek, vállalatok vagy szervezetek tulajdonában, illetve kezelésében vannak.

BARATSAGOSINTERNET

A Barátságos Internet Fórum segít a szülőknek az internet megértésében:
www.baratsagosinternet.hu

INTERNETOMBUDSMAN

Legyünk jártasak a virtuális világban és ismerjük jogainkat:
www.internetombudsman.hu

INTERNETHOTLINE

Az internet-forródrót webes és telefonos bejelentési lehetőséget biztosít illegálisnak vagy ártalmasnak ítélet magyarországi weblapok és online tartalmak bejelentésére:
www.internethotline.hu

Az internet-forródrót hívószáma:

06-1-487-60-50

SAFERINTERNET

Az Insafe az e-biztonság fontosságára hívja fel a figyelmet, melyet részben az Európai Bizottság finanszíroz. Nemzeti információs központjai az Európai Unió országaiban, illetve Izlandon és Norvégiában találhatók. Az Insafe célja, hogy a felhasználókat az Internet pozitív lehetőségeire bátorítsa és megmutassa, hogyan lehet elkerülni a potenciális veszélyeket:
www.saferinternet.org

ins@fe

A UPC Magyarország támogatásával
www.upc.hu

Cím: Családi e-biztonsági csomag • Készítette az Insafe, a Liberty Global/UPC támogatásával, 2008-ban