

Csizmazia-Darab István [Rambo]



SZÜLŐK KÖNYVE

Csizmazia-Darab István: Szülők könyve
Útmutató a digitális világhoz szülőknek és pedagógusoknak

Készült: 2016.

A BIZTONSÁGOSABB INTERNET KÖZÖS ÜGYÜNK

"Ha egy évre tervezel, ültess rizst; ha húsz évre tervezel, ültess fákat; ha a következő generációknak tervezel, tanítsd az embereket." (kínai közmondás)

Tartalomjegyzék

0. fejezet: Előszó

1. fejezet: Amit a szülőknek is tudnia kell(ene)

2. fejezet: Mit nem lát meg a legtöbb felnőtt?

3. fejezet: Média és médiaértés

4. fejezet: Hasznos és káros tartalmak az interneten

5. fejezet: E-mailezés, jelszavak

6. fejezet: Közösségi oldalak, digitális lábnyom

7. fejezet: Chatelés, üzenetküldés, sexting

8. fejezet: Webkamera

9. fejezet: Vírusok, férgek, kártevők

10. fejezet: Lánclevelek, álhírek, spamek, csalások, átverések

11. fejezet: Cyberbully - online bántalmazás, zaklatás

12. fejezet: Szexuális bűnözők

13. fejezet: Bankolás, online vásárlás

14. fejezet: Informatikai higiénia

15. fejezet: Mobiltelefon

16. fejezet: Mobileszközök - okostelefon, tablet

17. fejezet: Játék, játékkonzolok, okos tévé

18. fejezet: Függőség, szenvedélybetegségek

19. fejezet: Kihez fordulhatunk

20. fejezet: Tudatos szülői hozzáállás

21. fejezet: Tudatos gyermeki hozzáállás

22. fejezet: Tudatos pedagógusi hozzáállás

23. fejezet: Szótár, szómagyarázatok

24. fejezet: A szerző bemutatása, ajánlott weboldalak és szakirodalom

25. fejezet: Képanyagok

0. fejezet: Előszó

Kulcsszavak: y-generáció, alfák, online élettér

Tények: Ezt történik az interneten 1 perc, azaz 60 másodperc leforgása alatt a 2014-ben megjelent „Data Never Sleeps 2.0” jelentés szerint: 204 millió e-mail üzenetet küldenek, 2 millió 460 ezer megosztás keletkezik a Facebookon, 347 (ez 2015-ben már 277) ezer Twitter üzenet jön létre, 216 Instagram posztot készítenek, 300 (ez 2015-ben már 72) órányi videóanyag kerül feltöltésre a YouTube videó portálon, 4 millió Google keresést indítanak a felhasználók világszerte, és 590 (ez 2015-ben már 416) ezer jobbra vagy balra húzással döntenek a Tinder társskeresőjében arról, hogy szimpatikus-e valaki. Az USA-ban a 3-4 éves gyerekek 6.5 órát töltenek az internet előtt hetente. Később az 5-7 éveseknél ez már 9.2 órára nő, míg a 8-11 évesek még többet, 17 órát neteznek hetente. Argentínában 2013.-ban, a "grooming" és "internetes zaklatás" fogalmát beépítették törvénykezés szövegébe. Sok már országban azonban még sajnos nem tartanak itt.

Kedves Szülők!

Az internet egy nagyszerű dolog, a XX. század legnagyobb forradalmi vívmánya. Sokkal több előnye van, mint kockázata. Kényelmes, erősíti a szociális kapcsolatot, segít a probléma megoldásban, tanít. De mindenkinek tisztában kell lennie a veszélyeivel is. Hogy hogyan kell nevelni, jól nevelni egy gyereket, azt nem tudjuk mindig pontosan megmondani. A Mézga rajzfilm „Üzenet a jövőből” cím mintájára mi azt mondhatjuk, hogy a gyerek „üzenet a jövőbe”, aminek a hatásait nem tudjuk, még nem ismerjük.

A számítógép, az internet nem bétiszitter. A tapasztalatok azt mutatják, hogy gyermekeink egyre fiatalabb korban kezdenek számítógépes, internetes eszközöket - okostelefon, tabletet, noteszgépet, játékkonzolt - használni. Egy friss, 2015-ös tanulmány pedig arról számol be, hogy eközben minden ötödik szülő semmit sem tesz gyermeke biztonsága érdekében, valamint a szülők 58%-a egyáltalán nem beszél velük az online veszélyekről, fenyegetésekről.

Egy 2015-ös felmérés szerint a brit szülők 54 százalékának fogalma sincs arról, ha a gyermekét az interneten keresztül zaklatták. Ez azt is jelenti, hogy a legtöbb szülőnek nincsenek a kezében megfelelő eszközök, hogy időben felismerje és kezelje ezt a gyerekekre egyre gyakrabban leselkedő problémát. A hazai helyzet hasonló, az ismeretek hiánya mind a szülők, mind pedig a gyerekek részéről egyaránt komoly problémákat okoz.

Kérjük, figyeljenek oda gyermekükre. Ne tiltsuk a használatát, mert az nem megoldás, de mindenképpen alakítsunk ki ésszerű használati szabályokat! Emellett pedig ahogy jó esetben azt is megbeszéljük, hogy mi volt az iskolában, mi volt a foci edzésen, a táncórán, vagy a rajzsakkörben, úgy azt is rendszeren kérdezzék meg, mi történt ma az online

világban. Az érdeklődésre és az érzelmi támogatásra akkor is meg tudják adni gyermeküknek, ha nem számítógépes szakemberek. Azt ugyanis lehetetlen megakadályozni, hogy böngészés közben ne botoljunk bele nem kívánt tartalmakba, a vírusírók sem fognak sajnos felhagyni kártevőik terjesztésével, és a csalásra szakosodott bűnözők, pedofilok is egyre jobban kihasználják a számítógépes világháló nyújtotta lehetőséget.

Azt azonban szükségesnek tartjuk, hogy a gyermekek életében kulcsfontosságú szerepet betöltő minden szereplőnek - így a gyerekek magának is, de emellett a tanároknak és a szülőknek is - tisztában kell lenni, hogy az internet számtalan nagyszerű előnye mellett milyen veszélyeket rejt. Ha ezzel mind a gyermek, mind a felnőtt tisztában van, azt is tudják, hogy ijesztő, félelmetes vagy zavaró szituációkban mit tehetnek, hova fordulhatnak segítségért, akkor már ez az összefoglaló elérte a célját. A gyermekek oktatásán azt a szoktuk kihangsúlyozni, hogy a saját tudásuk lesz a legjobb védelem. Ezt felhasználhatják abban is, hogy már tudják, hogy erről ne hallgassanak és kihez forduljanak, ha problémájuk támad. De természetesen azt is fontos megérteniük, hogy némely területen - ilyen például az iskolai zaklatás (cyberbullying) - nekik is van feladatuk, mégpedig az hogy ne hagyják bajban egyetlen társukat sem, vigyázzanak egymásra. Kérjük, Önök is tájékozódjanak rendszeresen az internetes veszélyekkel kapcsolatban, hogy naprakész tudásukkal, empátikus hozzáállásukkal segíthessék gyermekeiket, akik már teljesen más világban élnek, mint szüleik: hiszen nekik a internet már nem eszköz, hanem élettér.

A közönyösség és a tudatlanság ellen vívott keresztes szélmalomharc ez a jó ügy érdekében, hogy véletlenül és akarata ellenére egyetlen gyerekkel se történhessen rossz dolog az interneten. Erre pedig minden szereplő jóakarására, figyelmére és folyamatosan gyarapodó tudására szükség van.

A könyv szerkezete szerint a következőképpen épül fel. Az első három fejezetben megmutatjuk, milyen helyzetben élnek azok a fiatalok, akik már beleszülettek a média világába. Milyen mintákat követnek, néhány extrém példával azt is megmutatjuk, milyen veszélyekbe csöppenhetnek, ha a szülők valamilyen ok folytán nem képesek nekik segíteni, illetve a problémáikat megbeszélni.

A következő fejezetekben az egyes tématerületek és az ott jelentkező ismereteket és veszélyforrásokat tekintjük át, amit minden egyes fejezet végén olyan gyakorlati példákkal, iránymutatásokkal, praktikus tanácsokkal is kiegészítünk, amelyekkel védekezni lehet.

Végezetül a könyvben szereplő rövidítéseket, szakkifejezéseket szedtük csokorba rövid, de érthető magyarázatokkal, és mindezt az ajánlott weboldalak és szakirodalmak listája zárja.

"Tökéletes védelem sajnos nincs. Ha a felhasználó képzetesebb, akkor a védelem is eredményesebb"

(Szőr Péter 1970-2013, víruskutató)

„Ha nem ismered a bűnt, elkövetik ellened, hogy megismertessenek vele.” A számítógépes biztonságban van egy kimondott és nagyon erős törekvés: legjobb védekezési módszer a megelőzés. A felnövekvő generációk hatékony megvédése szerintünk sokban múlik azon, időben át tudjuk-e adni számukra azokat az ismereteket, amelyek birtokában majd képesek lesznek szembenézni a veszélyekkel, meg tudják védeni magukat és társaikat.

Ehhez a küldetéshez információval már teli a padlás, sokkal inkább a tudás hiányzik a fejekből. A kiadványban ismertetett veszélyek, esetek célja nem az ijesztgetés, hanem a valósággal való őszinte szembenézés. Hiszük és valljuk, hogy az üdvözítő megoldás mindig az említett megelőzésben, a megfelelő és folyamatosan naprakész tudásban rejlik. Egy klasszikus Martin Seligman idézet szerint: „Ez a fő tanulsága az utolsó évszázad közegészségügyi intézkedéseinek: a gyógyítás bizonytalan, de a megelőzés rendkívül hatékony - például, amint előírták a bábáknak a kézmosást (fertőtlenítővel), megszűnt a gyermekági láz, vagy például az oltás véget vetett a gyermekbénulásnak.” Úgy gondoljuk, hogy a következő tudatformáló ismeretek ugyanígy segítenek eligazodni az internetes világunk veszélyei között úgy, hogy a benne rejlő végtelen és nagyszerű lehetőségeket biztonságosan élvezhessék gyermekeink.

Végül következzen egy a mai helyzetet jól szemléltető idézet Mérő László professzortól: „A régmúltban olyan volt a világ, hogy többé-kevésbé ki lehetett számítani matematikailag. Most olyanná válik a világ, hogy matematikailag bebizonyítható: nem számítható ki egy csomó jelensége. Márpedig, ami nem számítható ki, arra nem tudunk felkészülni és felkészíteni közvetlenül. Ezért fontos az, hogy közvetve készüljünk fel, hogy olyan tudást nyújtsunk, ami jó eséllyel olyan problémák megoldására is alkalmas lesz a jövőben, amiről ma még azt se tudjuk, hogy ezek valójában problémák.”

Tenni akartunk valamit, reméljük sok hasznos ismeretet sikerült átadnunk. "Többet használsz azzal, ha gyújtasz egyetlen gyertyát, mintha egész álló nap az Edison társaságot szidalmazod."

Mindenkinek hasznos olvasgatást kívánunk: a szerző

1. fejezet: Amit a szülőknek is tudnia kell(ene)

Kulcsszavak: generációs különbségek, állandó online jelenlét, közösségi oldalak, megosztás

Tények: A life.hu közösségi oldal így fogalmaz az internetes, okostelefonos modern világban élő gyerekekről: "Ha késve érnek haza, csak dobnak egy sms-t, az iskola legszaftosabb pletykáit pedig Viberen vagy Messengeren keresztül beszélnek meg az éj leple alatt ágyukból a barátnőikkel. Tízévesen pózolnak és posztolnak, szomjazzák az elismerést, csodáló tekintetekre vágnak, ezt pedig meg is kapják lájkok formájában, ami abba az illúzióba ringathatja őket, hogy értékesebbek, fontosabbak társaiknál."

Manapság nem könnyű gyereket nevelni, tanítani. Egészen más körülmények között nőnek fel, mint szüleik, vagy mint a mi szüleink. A régebbi játszótéren zajló élő játék, az akkori kevés technikai eszköz, nagyságrendekkel kisebb szórakoztató ipar, a hétfői adásszünetes fekete-fehér televízió a kettő-három csatornájával nem befolyásolta annyira a szokásokat, nem terelte el a figyelmet a napi teendőkről. Eközben pedig nekünk felnőtteknek is megváltozott az életünk, például a munkával töltött idő is emelkedett. Nem ritka a hazavitt feladat, a túlóra, a munkával töltött hétvége, önként vagy vállalati keretek között végzett továbbképzések-tanfolyamok is rendszeresen lekötik szabadidőnket, nem is beszélve a vállalkozói létről, ami sokaknál a 10-16 órás munkanapokat jelenti. Emiatt viszont a családdal, gyerekkel töltött "minőségi" idő is sajnos lecsökkent, például a magyar szülő naponta átlag 7 percet beszélget a gyerekével.

Bár fontos, hogy kik vagyunk-voltunk mi 30-40-50-es szülők, ám emiatt az idő nem fog visszafordulni, és a fejlődés és a változás sem fog megállni. Az igaz, hogy "bezzeg a mi időnkben" a maihoz képest szigorú poroszos nevelést kaptunk, hogy akkor a felnőtteknek még nagyobb tekintélye volt, létezett még kütyünyomkodás nélküli beszélgetés, a gyerekeknek még volt valódi gyerekora, és mi még zömmel biciklit, labdát és babát kértünk karácsonyra.

Ehhez képest most sokszor nem értjük a fiatalabb generáció viselkedését, a felnőttnek nincs tekintélye, nem is akarnak tőle tanulni, a gyerekeink még egy szobában ülve sem beszélgetnek, hanem inkább a kütyükön irkálnak egymásnak és ők karácsonyra már okos telefont, tabletet, notebookot és játékkonzolt kérnek. Az is új helyzet, hogy a gyerekek az iskolában állandó versenyhelyzetben vannak, míg a mai felnőttek első nagy megmérettetése jobbra csak a 18 éves korban történt érettségi vizsga volt.

A korábbi generáció még Columbo, Bud Spencer, Star Wars műsorokat látott a televízióban, a hagyományos ismeretek miatt a szülőknek is nagyobb volt tekintélye, kamaszkorban szolid berúgásaink voltak, nem volt probléma a munkába állás, és például az esetleges megszegések szűk körben történtek.

Ehhez képest mi várja most a mai gyerekeket a televízióban? Horrorfilm, zombifilm,

vérfarkas, vámpír, Hannibal Lecter, Dexter, Narancsvidék, Trónok harca és más sorozatok dömpingje. Egy Rém rendes család, vagy Férjek gyöngye sorozat epizód megtekintése után milyen egy apa figura megítélése? De más területeken is észlelhetők erőteljes eltérések, változások. A mai 30-40-50-es generáció ha fiatal korában alkoholt ivott, jól akarta magát érezni. Ezzel szemben sokszor tapasztaljuk - ezt Zacher Gábor nyilatkozatai megerősíteni látszanak - a mai fiatalok önpusztítók és azonnal öntudatlanra akarják kütni magukat alkohollal, droggal. Sajnos az egyre fiatalabb korban kezdődő versenyszínpad is nehezíti gyermekeink életét, például a pályakezdők - de manapság már az idősebbek is - százasaival küldözgetik az önéletrajzot hónapokig, évekig. És ami még óriási különbség - erről részletesebben lesz a szó a zaklatásról szóló fejezetben - a megszegésének óriási nyilvánossága, amely akár egy életre ellehetetleníti az áldozatot

Az internet veszélyei szempontjából kétségtelenül a legkiszolgáltatottabbak a gyerekek. Ez az a generáció, aki a legtöbbet van online, a legtöbbet chatel, a legtöbbet közösségi oldalazik (Facebook, Instagram, Whatsapp, Pinterest, Twitter, Ask.fm, stb.), a legtöbb személyes információt osztja meg, a legtöbbet böngészik, a legtöbbet használja naponta mobileszközeit. Ám eközben általában nem rendelkezik kellő érettséggel, tettei következményeinek belátásával, szükséges óvatossággal, és ráadásul érzelmileg erősen sebezhető.

Mit rontott az egyre több online jelenlét? Kevesebb és felszínesebb lett a személyes kapcsolat, kevesebb élő beszélgetés történik, a hiányzó szemkontaktus talán szintén sokaknak feltűnhet, és azt is láthatjuk, hogy ebben a korosztályban kevesebb lett a könyv olvasás. A netes kapcsolatok miatt sokaknál jelentkezik az állandó visszaigazolási igény, dicséret függés, narcisztikus jellemvonások és hamis önkép alakul ki, agresszióra azonnali önkontroll csökkenéssel, öngyilkos gondolatokkal reagálnak, de ezzel párhuzamosan megfigyelhető a fokozódó agresszív hajlam, és a hiányzó büntudat is. További járulékos mellékhatás lehet a számítógép, illetve internet függőség kialakulása, a hiányzó jövőkép, és nyomasztó lehet még számukra "az internet nem felejt" terhe is.

2009-ben Hanula Zsolt az Indexről volt olyan kíváncsi, és utánanézett olyan alapkérdéseknek, mint "Tényleg megtartja az Iwiw és a Facebook a törölt képeket?", vagy mi történik azokkal a leveleinkkel, amiket látszólag törölünk? "Törölt levelek nyomában a neten" címmel. Nos, a törlések fizikailag sosem történnek meg azonnal, ha meg történnek egyáltalán. Ha valaki ismeri azok korábbi linkjét, még hónapokkal-évekkel később is meg tudja jeleníteni, illetve volt, ami nem hogy késve, de sosem tűnt el véglegesen. Ami az internetre egyszer felkerül, annak annyi. Az akváriumból lehet halászlét csinálni, de a halászléből már nem lehet akváriumot.

A felnőtteknek, tanároknak, szülőknek is muszáj megértenie az életünkben bekövetkező változásokat, tanulni és kezelni kell a változásokat, valamint nekik is meg kell tanulniuk a biztonságos internethasználatot.

A tanárok közt is van generációs konfliktus: A kőszívű ember fiai vagy Harry Potter legyen a kötelező olvasmány? Hagyományos vagy számítógépes legyen a tanítás? Mert azt nem

tehetik meg, hogy egyáltalán ne értsenek az internethez, mert akkor nem képesek megvédeni a gyermekeket.

Miért van szükség gyermek oktatásra? Jelenleg csak számítástechnika van 5. osztálytól, műszaki reáltárgyként. Az évi egy ezzel a témával, és külső előadóval lebonyolított osztályfőnöki óra meghívásra - jó esetben nagyon kevés az érdemi információk átadására. Emellett a tantestület nincs felkészülve, a ma már minden magyar iskolában is jelentkező zaklatásos eseteket egyedileg, ad hoc jelleggel oldják meg, igaz erre egységes segítő útmutató sajnos nem is létezik. Tapasztalat szerint a SIP előadásokra rácsodálkoznak és utólag nagyon örülnek neki.

Ha a számok mögé nézünk, hány embert is érint mindez, akkor azt látjuk, hogy a 2014/2015-ös tanévben az általános iskolai tanulók száma 748,500 fő volt, ezalatt a köznevelésben az iskolák száma 10,829, míg a köznevelésben foglalkoztatott pedagógusok száma 153,000 fő volt.

Minden diáknak készség szinten tudni kellene: mik a veszélyek: vírusok, kémprogramok, webkamerás kukkolás, átverések, iskolai zaklatások, stb. Az is fontos, hogy képben legyenek, milyen incidensek történnek világszerte, milyen következmények lehetnek, hogyan védekezhetünk ezek ellen, kihez forduljunk ha az interneten bajba kerülünk. Ezek az ismeretek EGYSZERRE etikai és számítástechnikai kérdések, oktatásukhoz mindkét képesség szükséges.

2. fejezet: Mit nem lát meg a legtöbb felnőtt?

Kulcsszavak: internet, függőség, Facebook, internetes zaklatás, veszélyek, ismeretek

Tények: 2014-ben a német informatikai cégek szövetsége (Bitkom) felmérést végzett. Ebből többek közt az derült ki, hogy a 6-7 évesek körében 76% alkalmanként, a 10 éves korosztályban viszont már 94% százalék internetezik. A tízévesek átlagosan 22 percet, míg a 16-18 éves korosztály tagjai pedig 115 percet töltenek internetezéssel naponta.
<http://sworld.hu/2014/05/07/nemetorszagban-mar-majdnem-minden-tizeves-internetezik/>

Egy 2015-ös felmérés eredménye szerint 10 szülőből átlagosan három mindenfajta megkötés nélkül engedi gyermekének, hogy használja az internetet. Mindeközben 100 tinédzserből 5 vallotta be, hogy a neten megismert személyekkel már személyes találkozót is megbeszélt, illetve egyharmaduk szenvedett már el valamilyen fokú zaklatást az online térben.

HELYZETKÉP

A helyzet évről évre rosszabb. Az incidensek, zaklatások esetén "az áldozat megszégyenül, és esetek 60-70%-ban nem mondja el a történeteket". Az Országos Gyermekegészségügyi Szolgálat 2010-es jelentése szerint a magyar gyerekek 15%-a elkövető, 13% esik áldozatául az iskolai bántalmazásnak, és úgy tapasztaljuk, hogy a helyzet évről évre súlyosbodik.
<http://mediamuhely.wordpress.com/2014/03/10/kiberzaklatas-kortars-pszichoterror/>

Mit nem lát meg a legtöbb felnőtt?

Sajnos sokan elektronikus dadának gondolják a tévét és a számítógépet, lepasszolják a gyerkőcöt. Semmit, vagy csak az időtartamát korlátozzák a használatnak, a tartalmát viszont legtöbbször egyáltalán nem. Ezalatt a gyerek egyedül az néz rajta, amit akar, így sajnos könnyen ütközhet életkorának nem megfelelő tartalmakba. A 2015-ös médiakonferencia szerint a 8-14 éves korosztály legnézettebb műsora az abszolút nem nekik való Éjjel nappal Budapest.

Minden korosztály már függő lett a netes kütyüktől (és ez már lassan az idősebbekre is vonatkozik. Ehhez elég szétnézni utazás közben a villamoson, buszon, metróban. Az olvasó egyszer mérje le a tv-zés, netezés, okostelefonozás napi idejét SAJÁTMAGÁNÁL, és garantáltan lesz meglepetés. Emiatt sincs értelme a "bezzeg a mi időnkben" közhelyeknek, arra a helyzetre kell megoldást találni, ami itt és most van. Ugyanis a gyerekek NEM AKARNAK másképp élni, ott kell őket megvédeni, ahol éppen vannak. Ám ehhez a felnőtteknek is kell(ene) élethosszig tanulnia.

A valóság szomorú és brutális. Részletek egy 2013-as cikkből. „Az ask.fm nagyon pörög most a tizenévesek között. Mintha direkt arra találták volna ki, hogy a trollok gyalázkodjanak rajta: a felhasználók itt bárkinek a kérdéseit megválaszolják. A kérdések sokszor durvák. Több felhasználója öngyilkos lett.” Egy gyermekvédelmi konferencián egy pszichológusnő előadásából pedig az derült ki, hogy emiatt a magyar gyerekek

negyedének megfordul a fejében az öngyilkosság gondolata.

A számítógépes ismerkedéssel kapcsolatos bűncselekmények közül az egyik legsúlyosabba, amikor az elkövetők tömegesen próbálnak fiatal lányokkal ismerkedni, hasonló korúnak kiadva magukat és szerelmet, érdeklődést tettetve, majd a személyes találkozás alkalmával egyszerűen elrabolják a tinilányokat és eladják prostituáltként. 2013-ban volt egy interjú egy gyermekvédelmi szakemberrel, aki a joghézagok, és a hosszú ideig tartó bírósági, kiadatási eljárások miatt kétségbeesésében személyesen „lopja haza”, gyakran életveszélyes kalandokba keveredve a bajba került, fogvatartott lányokat. "Hány éves volt a legfiatalabb lány, akit hazahoztál? A legfiatalabb egy tizenkét éves heroinfüggő Hollandiából. Évekkel ezelőtt ketrecharcosokkal beszélgettem a munkámról, és mondták, ha legközelebb megyek, szóljak. Nagyon sokat köszönhetek nekik, jóval többet, mint bármelyik rendőrkapitánynak."

http://velvet.hu/sztori/2013/08/02/interju_a_gyermekvedelmissel/

Szerencsére nem csak ilyen végletes események történhetnek, de rossz hatások már egészen kis gyermekkortól érhetik például a mesefilmet néző óvodás-kisiskolás korosztályt. Részlet egy közösségi oldalon megjelent posztból, amit a szülő osztott meg: *"Kislányom kérte, hogy C***** N*****-öt nézhessen. Nem tudtam, mire bólintok rá. Szemelvények egy negyed órás GYEREKEKNEK SZÁNT, korhatár nélküli rajzfilmből. Sajnos, így is változik a világ.*

- *Genya vagy.*

- *Ne szívass!*

- *Na húzzunk bele abba a lejárató kampányba!"*

A gyermekekkel foglalkozó szakemberek szerint egyértelműen kimutatható, hogy egyre gyengülő szolidaritás, együttérzés, egyre több közömbösség tapasztalható, illetve a megnyilatkozásokból - verbálisan és írásban is - túlteng a negatív kritika.

Ez többek közt a kommentek, vagyis a megjelent cikkek, blogposztokra írt megjegyzések kapcsán is erőteljesen észlelhető. Az még a jobbik eset, ha a helyesírását kritizálják a posztírónak, de sokszor a különféle esetek, incidensek kapcsán az áldozat felé semmilyen együtt érző magatartást nem tanúsítanak, félinformációk alapján elítélik - „megerőszakolták? biztos ő tehet róla”, vagy ami még szokatlanabb és hihetlenebb, lázadóan egyenesen az elkövető pártját fogják. Egy Facebook-kal foglalkozó posztban, amely arról szólt, hogy nem határolódtak el pedofil tartalmaktól, hanem azt „viccesnek” tartották, az alábbi kommentek születtek:

"Támogatom a FB bátorságát, hogy szembe mer szállni a bulvármédiák pedofilhisztériájával. "

"A pedofiliek üldözése gusztustalan, felháborító."

Emellett a gyerekek stresszes helyzetét az is erősíti, hogy zajlik a korai versenyhelyzet: iskolában, versenysportban. „Állj be és versenyezz” - biztatják. Emellett pedig „az átlagos az rossz” - sugallják, csak a kiemelkedő, az első a jó.

3. fejezet: Média és médiaértés

Kulcsszavak: forrás kritika, információ, tudás, olvasás, média, televízió, mozi, letöltés

Tények: *Megszűnt a korábban megszokott könyv, fotó, újság, mozi fogalma, és ezek helyébe a legtöbb fiatalnál a számítógép, illetve a mobileszközök léptek. A fiatalok könnyen hozzáférnek az információhoz, de gyakran nem értik, nincs tudásuk, hogy ez igazából pontosan mit jelent, és nincs forráskritikájuk. A magyarországi televíziónézés nap átlagos ideje 4 óra 4 perc.*

Az Ofcom 2015-ös felmérésében a kutatók arra voltak kíváncsiak, hogy a fiatalok különbséget tudnak-e tenni a netes keresések során született találatok között. Az eredményből kiderült, hogy a 12-15 éves korosztálynak csak harmada ismerte fel a fizetett Google hirdetéseket, míg a kisebb, 8-11 éves gyerekek közül mindössze egyötöde értette, hogy a kapott találatok között melyik miért jelent meg. A pedagógusok szerint a gyerekek szóincse egyre szűkül, jelentős részük egyáltalán pedig egyáltalán nem olvas könyveket.

2014-es adatok szerint a YouTube több amerikai felnőttet ér el 18-34 év között, mint bármely TV hálózat.

Neil Postman A gyermekkor eltűnése (The Disappearance of Childhood) című könyvében azt írja, hogy „egyedül a számítógép lehetne olyan kommunikációs technológia, mely a gyermeki lét iránti igényt szolgálja, ezen belül a programozás ugyanis ismét előtérbe állíthatja a komplex nyelvismeret kikerülhetetlenségét, de féltő, hogy a tömegek számára csak a gondolkodás nélküli zeneletöltés, reklámfogyasztás, pornó és lövöldözősdi jelent számítógép-használatot.”

A média többet nevel, mint az iskola vagy a szülők. Emiatt a gyermekek médiafogyasztását érdemes szabályozni, keretek közé szorítani. A korhatár jelzések lényeges elemei lennének a televíziós és mozi műsornál, valamint játékszoftvereknél, de sajnos sokan ezt figyelmen kívül hagyják. Például a televízió nézés statisztikája lehet, hogy sokakat meg fog lepni. A Nielsen adatai szerint 2015 negyedik negyedében a teljes népesség naponta átlagosan 5 óra 2 percet töltött a tévékészülékek előtt, amely 2 perccel volt több, mint az előző év ugyanezen időszakában. A 4-17 évesek tévénézéssel töltött ideje 3 óra 28 perc volt, a 18-49 éves korcsoporté pedig 4 óra 5 perc, ami a gyerekek esetében 1 perces, míg a 18-49 éveseknél 6 perces csökkenést jelentett. Az 50 évnél idősebbek naponta átlagosan 6 óra 41 percet tévéztek az év utolsó negyedében: 11 perccel többet, mint egy évvel korábban.

Az életkornak megfelelő tartalom nagyon fontos: TV műsor, internet, vásárolt játékprogram, ebben is jelen van a szülők felelőssége. Amíg a felnőtteknek a számítógép, az internet csak eszköz a céljaihoz, addig a gyerekeknek a számítógép, az internet az ÉLETTÉR. Ahol a durvaság, trágárság szóban vagy írásban is nagyon lehangoló, zavaró. A vizualitás vagyis a látás a legnagyobb hatású, és egy felnőtteknek való, vagy akár egy jó érzésű felnőtteknek sem való kép, videó tartalom napokra sokkolhatja őket, ha ilyenbe véletlenül belefutnak, amire azért jó esély van. Az itt felbukkanó veszélyek elég erőteljesen meg tudják érinteni, ijeszteni őket: gyermekpornográfia, drogkereskedelem,

pedofilok, zaklatók, erőszak, öngyilkosságok, stb. Akkor védhetjük meg őket hatékonyan, ha rendszeresen beszélgetünk vele az online életéről is.

Ismerjük meg a korlátozásokat végző lehetőségeket

Mindannyian olvastunk már rémtörténeteket arról, hogy időnként a gyerekek elárult jelszó miatt az horror összegben vásárolt az eredetileg ingyenes okostelefonos játékon belül fizetős játékkiegészítőket. A címlapos sztorikban "a szülő beperli az Apple-t" szalagcím inkább szánalmas, mint követendő. Felelős szülőként nekünk illik a jelszót nem elárulni, a szükséges képernyőzárolásokat beállítani, illetve a játékokon belüli vásárlási lehetőségeket letiltani iPhone, iPod, iPad, és egyéb kutyukon, így elkerülhetjük a "számlasokkot". Amiben viszont mégis jogosan háboroghatnak a szülők, hogy ennek alapértelmezett állapota miatt az engedélyezett. A válasz erre az, hogy pontosan ugyanazért, amiért a Facebookon is default a megosztás a mindent mindenkiével ;-)

Hogyan juthatunk médiatartalmakhoz? A magyarországi szabályok szerint a magáncélú média - zene, film - letöltés, jogszerű. Tehát ha nem adom oda másnak, saját célra töltöm le, akkor igen. Ám a torrentezés - ahol a kicsiny fájlszeletekből ami nálam már letöltődött, azt mások tőlem töltik le, emiatt én is feltöltővé válok - nem az. Ez tehát a szabály, igaz nem láttunk még senkit a híradóban, hogy bilincsben verve vitték volna el torrentezés miatt. Nem árt tudni, hogy külföldön viszont néha akcióba lendülnek a szerzői jogvédők, lekérlik a felhasználók listáját az internetszolgáltatóktól és csoportos pereket kezdeményeznek. Néha elképesztő összegeket számolnak ki egy-egy MP3 számra, vagy például a Bombák közt című film kapcsán is történt egy ilyen pereskedés. Egy nagyon alapos összefoglalót lehet olvasni az internet „Használati útmutató a digitális jogkezeléshez” címmel, ebben sok ezzel kapcsolatos kérdésre választ lehet találni.
http://www.indicare.org/tiki-download_file.php?fileId=197

Érdekes egyébként az a 2016. májusában született határozat, melyben a Kúria szerint a letöltők személyes adatainak védelme erősebb érdek, mint a reklamáló kiadók felhasználókat azonosítani kívánó, szerzői jogokat megvédeni kívánó procedúrája. Erről így számolt be az Index cikke: "A határozatban meg nem nevezett felperes azt akarta elérni, hogy az egyik (szintén anonim) internetszolgáltató adja ki a megadott hálózati azonosítókhoz (IP-címekhez) tartozó előfizetők nevét és címét, mert azok szerinte jogosulatlanul töltötték le és osztottak meg szerzői jogi védelem alatt álló filmeket. A Kúria azonban egyetértett a jogerős ítéletben foglaltakkal, miszerint a szolgáltató sem előfizetői szerződések, sem az elektronikus kereskedelemről szóló törvény értelmében nem köteles kiadni az előfizető személyes adatait a hozzájárulása nélkül. Sőt, a Kúria azt is kimondta, hogy ezeket az adatokat a szolgáltató nem csak hogy nem köteles, de nem is adhatja ki."

4. fejezet: Hasznos és káros tartalmak az interneten

Kulcsszavak: szűrőprogram, életkornak megfelelő tartalom, életkor, korhatár, keresés, letöltés

Tények: Egy 2015-ös kérdőívre az USA-ból és Kanadából kérdeztek meg összesen 1230 szülőt gyermekvédelemmel kapcsolatos kérdésekben. Ebből többek közt az is kiderült, hogy öt szülőből négy szerint van rendben az, ha a szülői felügyeletet biztosító szoftvert telepítenek a gyerek gépére anélkül, hogy arról a gyerek tudna.

"A kereskedelmi célú trollkodás történetét a legszebben a globális vendéglátóiparban meghatározó Tripadvisorral lehet bemutatni. A 2000-ben alapított, a felhasználók beszámolóira épülő oldal egy évtized alatt igazi szörnyűvé nőtt, amellyel egy pillanat alatt lehet romba dönteni vagy az egekbe emelni éttermeket és szállodákat. 2015. júniusában a BBC egyik műsorában hangzott el, hogy az angol oldalakon az állítólagos felhasználói beszámolóknak legalább 20 százaléka kamu."

„A gyermekek netes keresésénél Németországban és az Egyesült Királyságban az alkohollal, dohányossal és kábítószerrel kapcsolatos oldalak vezetnek (23 és 25 százalékkal), míg Kínában és Japánban a felnőtt tartalmak keltik a legnagyobb érdeklődést (23 és 5 százalék). Ez a kategória egyébként az angol és amerikai fiataloknál a legnépszerűtlenebb (kevesebb mint 1 százalék)."

„A látványosan csomagolt dolgokra kattintunk, mert ez az evolúció parancsa.”
(Hanula Zsolt)

Mik lehetnek ezek az úgynevezett korának nem megfelelő tartalmak. Igen sokféle kategóriát ide sorolhatunk, a durva, erőszakos, trágár beszédet, szöveget, a direkt agressziót, öngyilkosságra való buzdítást, szélsőségesen agresszív vagy beteges játékokat, videókat, az abortuszról, szektákról, öncsonkításról, a reális testképről való megtévesztő beszámolókat, a pornográf képeket, videókat, pedofilokkal történő csevegőszobákat, és a sor hosszan folytatható. Emellett fontos tisztában lenni azzal is, hogy egy információ, attól, hogy „az interneten található”, még egyáltalán nem biztos, hogy igaz is. Tehát lényeges, hogy különbséget tudjunk tenni hiteles és hiteltelen információk között.

Vannak viszont olyan weboldalak is, amelyek szélsőségesen diszkriminatív, sértő, pejoratív, megszégyenítő, kirekesztő tartalmak közlésére specializálódtak (puruttya, pedomaci, agyiszint, stb. weboldalak), de ahogy mindennek, ennek is meg van a maguk fogyasztó közönsége.

A „hol ütközhetnek a gyermekek ilyen tartalmakba” kérdésre számtalan válasz létezik. Bárhol. Például hiába rendelkezik a családi számítógép szűréssel, ha a gyermek mobilneten néz meg valamit, vagy átmegy a barátjához internetezni. Szokás, hogy egymásra rálicitálva meghökkentő, ijesztő tartalmakat mutatnak a másikat. De a számítástechnika óra sem kivétel ez alól, hiszen a szünetben a kisebb gyerekek sokszor horror és egyéb videókat mutathatnak egymásnak, mert ez a terem közös a középiskolásokkal, és emiatt nincs benne semmilyen szűrés, vagy korlátozás.

A pornográf oldalakra való bejutás technikailag sem probléma egy gyereknek, hiszen jelenleg a legtöbbször az adott oldal felajánl két lehetőséget: elmúltam 18 éves; még nem múltam el 18 éves.

Vajon képesek-e a felhasználók felbecsülni, hogy milyen nyomokat hagynak az interneten? Röviden: nem igazán. Van persze ennek egy egyszerűbb vetülete, ha például úgy közelítjük meg, vajon mit tud rólunk a Facebook? Viccesen azt is válaszolhatnánk arra, hogy amit beírtunk neki. Ha valaki veszi a fáradságot, és az Általános beállítások menüpontban letölti az eddigi összes aktivitását egy tömörített állományban, csodálkozhat vagy elégedett lehet magával - mindenesetre ezt egyben látni nagyon tanulságos. (Zárójelben ott olvasható az összes eddigi bejelentkezési IP címünk is.) Ahogyan az is, ha a Facebook Graph Search keresővel családi állapotra, vallási hovatartozásra, pártállásra, érdeklődési körre keresgélünk, elképesztő, hogy milyen széles körben megosztott információ halmazba ütközünk.

Aztán lehet ezt úgy is szemlélni, hogy vannak nem is kevesen, akik eléggé "talkative"-ek, kitarulkozók és mindent megosztanak magukról, jellemző ez főként a nagyon fiatalokra, de később kortól függetlenül a kevésbé biztonság tudatos felhasználókra. Itt lehet tanulságos incidensekről, esetekről mesélni, hogy a bűnözők döntő többsége már használja a betöréseknél a közösségi oldalak nyújtotta könnyen és nyom nélkül hozzáférhető információkat. Ez például már egy 2011-es brit felmérésnél is 80% volt. Ugye ezért nem közvetítjük életünket percre készen a Foursquare-en, melyik sarkon fordulunk be, nem tudósítunk real time a reptéri becsekkolásainkról, nem jelentjük be előre a Facebookon ha nyaralni készülünk, vagy fényképezzük le a lakásunkat, műszaki cikkeinket, családtagjainkat. A manapság divatos mindent mindenkivel megosztási mániát én személy szerint nem tartom ésszerűnek, talán azért is, mert a szakmából kifolyólag sok negatív hatást látok. De persze nem mehetünk el amellett sem, hogy a közösségi oldalak alapértelmezett biztonsági beállításai is szándékosan a kitarulkozást szolgálják, nekünk kell - rendszeresen - opt-out megnyirbálni, állítgatni ezeket.

Ez eddig persze szép és jó, és még ha betartjuk is szépen ezeket, akkor ott van az, ha valamilyen ismerősünk viszont nem, és a közös képekről ő úgy gondolja, hogy lefotózunk, felcímkézünk, kiteszünk. Illetve különféle eszközökkel, API függvényekre támaszkodva még a Graph Search keresőnél is hatékonyabban lehet kényes információkra vadászni: szexuális orientáció, droghasználat, csalás a vizsgákon, házastársi hűtlenség, stb. Az ilyen előbányászott lejáratosokra remek példákat láthatunk a választási kampányok időszakában. Ebből a szempontból - ha csak ugye nem az említett jó ismerős tölt fel rólunk suttyomban - az van biztonságban, amit fel sem töltünk. Sosem tudhatjuk, milyen munkakörre fogunk jelentkezni tíz év múlva, és a most még viccesnek gondolt "iszunk-hányunk-belefekszünk" bulis fényképek a későbbiekben könnyen megghiúsíthatnak állásterveket, és azt se feledjük, ami egyszer felkerül a netre, azt már onnan nem lehet letörölni.

Nem beszéltünk még arról, hogy a keresők - például a Google - vagy úgy általában a különböző webhelyek milyen mennyiségű adatot gyűjtenek rólunk, szokásainkról, vásárlásainkról nagy buzgalommal mindezt állítólag azért, hogy testre szabottabb reklámokkal szolgálhassanak számunkra. De ennek ellenére szerintem nem az a megoldás,

hogy akkor bedobjuk a gyeplőt a lovak közé: ha úgy is fürkésznek, nincs mit tenni, meg az "én csak egy hétköznapi ember vagyok, ugyan mi bajom lehet ebből". Inkább alapos átgondolásra szorulna mindenki részéről a biztonságtudatosság - de persze ehhez az általános hozzáállásnak is nagyot kellene változnia.

Évek óta vannak olyan kifinomult csalások, ahol szándékosan hamis, fertőzött csomagokat tesznek fel a torrent oldalakra, és még csak az sem érdekes, hogy létező dologról van-e szó. Magyarán nem kell a Photoshop, Microsoft Office vagy Adobe Indesign ahhoz, hogy sikerrel járjunk, hanem gyakorlatilag nincs olyan eszement karakter sztring, amit begépelve ne jöjjön "találat". Ez jó módszer ez arra, hogy a naiv keresgélőket kéretlen reklámprogramokkal, kártevőkkel árásszák el. A lényeg, hogy a fájlmegeosztó oldalakon bármit keresünk, mindig lesz "találat". Lehet a keresés tárgya a "ashdfldsd76fas8fasjklkj" karaktersorozat is, de ha a próba kedvéért olyat gépelünk be, mint "A cecelégy bal lábbal kelt fel és Vegasba ment kelkáposztáért", ez a keresés is eredményes lesz. A tapasztalatok azt mutatják, hogy a kattintás után kiválasztható állományok valamilyen kártevőt, kém- vagy reklámprogramot igyekeznek ránk sózni. Ha a letöltött állományt megvizsgáljuk VirusTotal weboldalon, borítékolható, hogy a vírusmotorok többsége riasztani fog rá.

Gyakori eset az is, hogy neves, de egy bizonyos platformra még nem is létező szoftverek helyett tesznek fel trójaikat, ilyen volt például 2009-ben a Foxit for Macintosh, ahol a nem létező Mac változatot készítették el ismeretlenek, pedig hivatalosan Windows, Windows Mobile illetve U3 / Desktop Linux alá lett kifejlesztve. A rosszindulatú link pedig egy OS X-re írt kártevőre mutatott. De emlékeztet a Google Play áruházba ismeretlenek által feltöltött hamis UPC Távrögzítő alkalmazás is. 2012-ben felkerült az akkor még Android Marketnek nevezett hivatalos piactérre egy ismeretlenek által készített "UPC Távrögzítő" alkalmazás, a cég logójával. Több hónapon keresztül töltögették le az emberek, mire valaki észrevette. És hogy még egy jellemző módszert is említsünk, az is egy bevált átverési forma, hogy valamilyen nagyon várt új szoftver helyett még a megjelenés előtt hamisítanak egy fertőzött csomagot, ez történt például 2013-ban a Blackberry messenger for Android esetében. Szóval mindig érdemes elővigyázatosnak lenni a letöltésekkel.

Forráskritika

Az IT biztonságban (is) sokat számít, hogy mit hiszünk el, illetve hogy mit veszünk észre. A hoaxok, spamek, social engineering trükkök már mindennaposak lettek, hamis PayPal számlák, állítólagosan felfüggesztett banki accountok, hamis halálhírek, és egyéb trükkök formájában folyamatosan szembesülhetünk velük. Az vagy, amit elhiszel - mondhatnánk. E viccesnek ható mondat mindenek ellenére komoly problémákat képes okozni. A nagyszüleink, és szüleink "azt írta az újság", "de hát a rádióban is bemondták", sőt a "TV-ben is láttam" hiedelmei után azzal is érdemes tisztában lenni, hogy ha valamit az interneten találunk, az egyáltalán nem biztos, hogy igaz.

Például 2015-ben a nyitott modellű (bárki szerkesztheti) Wikipédia oldalain nagyszabású takarítási akciót végeztek, melynek során ezúttal 210 cikket töröltek a rendszerből. A nem engedélyezett információk terjesztése egyébként az oldal Felhasználói Feltételeinek

megsértését is jelenti egyben, így emiatt akkor 381 fiókot blokkoltak "jogosulatlan információk" közlése miatt. Itt a jogosulatlan szó nem csak fizetett reklámozást, szolgáltatások üzletszerű népszerűsítését, vagy szerzői jogvédelemmel védett anyagok illegális felhasználását jelentheti, hanem véletlenül vagy szándékosan hamis információk megjelentetését is. Az angol nyelvű Wikipédia oldalon egyébként a legtöbbet szerkesztett oldal címet George W. Bush profiloldala nyerhetné el, ám az is megfigyelhető, hogy az egyes országokban a választások előtti kampányokban különösen felpörög a politikusi életrajzokban való törölgetés, javítgatás, szépítgetés.

Összességében a Wikipédia igen megbízható forrásnak számít. A gyerekek informatikai biztonsági oktatásában azonban el szokás mondani, hogy ha valaminek utána akarnak nézni, ne higgyék el azonnal az első oldal tartalmát, hanem keressenek párhuzamosan több hivatkozást is, amely ugyanazt mondja. Ennek demonstrálására néhány érdekesebb esetet most felsorolunk, amelyben ismeretlen elkövetők - gyaníthatóan szándékosan - hamis információkat terjesztettek az interneten, és annyit előrebozsáthatunk, ezek mindenkinek korosztálytól függetlenül elég tanulságosak lehetnek.

2013. január

Öt esztendeig nem vették észre, hogy a Wikipédia egy nem létező háborúról szóló írást is tartalmaz. Egy alaposan kidolgozott 4500 szavas profi szócikk volt ez, illusztrációkkal, magyarázatokkal, amely 2007 és 2012 között élte zavartalan életét, és végül 2013 januárjában került az újságok címlapjára. A bejegyzés szerint az úgynevezett "Bicholim konfliktus" 1640 és 1641 között zajlott a gyarmatosító Portugália és India között, a harc célja pedig a "Goan függetlenség" kivívása volt. A konfliktus lezárása pedig egy állítólagos békeszerződéssel ért véget.

2013. szeptember

Az előző akció inkább csak a szerkesztők éberségét próbálgatta, de léteznek emellett sajnos kifejezetten gonosz megtévesztések is, amelyekben az elkövetők szándékosan kárt akarnak okozni a gyanútlan olvasóknak. Az egyik ilyen történetben azt a fals információt terjesztették, hogy ha az iOS 7-re frissítjük az iPhone telefon szoftverét, akkor az vízálló lesz, és ehhez egy pohár vízben álló készülék fotóját mellékelték. Persze ebben az esetben, hogy ezt valaki bevegye, kellett egy jó adag naivság is, bár mondjuk szülőként is más ezt megélni, ha a csemete emiatt jóhiszeműen próbára tette a nem kevés pénzért vásárolt telefonját.

2013. december

Veszélybe kerülhettek az Xbox One tulajdonosok, ha bedőltek annak a csalásnak, amely arról közölt információkat, hogy miképpen lehet 360-as játékokat is játszani az akkor éppen frissen megjelent játékkonzolon. Bár a Microsoft megerősítette az akkor érvényes tényt, hogy nem volt rejtett visszafelé 360-as kompatibilitás mód az Xbox One konzolban, mégis sokan bedőltek az átverésnek és a végrehajtott lépések segítségével jóvátehetetlenül "téglásították" a készüléküket.

2013. december

Hasonlóan kellemetlen szituáció volt az az Apple Macintosh csalás is, amelyik azt állította, hogy 2009. óta létezik OSX alatt egy rejtett opció, amelynek segítségével ingyen bányászhatunk Bitcoin. Itt is igaz a megállapítás, hogy nem jóhiszemű tévedésről, hanem szándékos átverésről van szó, amelyet csak azok tudnak idejében felismerni, akik például alaposan ismerik a *nix rendszerek belső működését. Ugyanis a begépelendő parancs nem virtuális valutát termelt, hanem rendszergazdai jogosultsággal a gyökérmappától kezdve minden állományt és mappát jóvátehetetlenül törölt a merevlemezről, ez utóbbi hatását videón is megcsodálhatjuk.

Az Immortal Games 2010-ben végzett egy kísérletet, hogy az emberek mennyire figyelmesen olvassák el a felhasználói licencszerződéseket (EULA). Az egyik játékukba azt is beleírták, hogy aki kattintással elfogadja, az eladja a lelkét. A végeredmény 7500 „eladott lélek” és egy mindezt bemutató tanulságos cikk lett. De hogy egy kis segítséget is adjunk a sokszor több ezer oldalas szerződések értelmezéséhez: létezik egy EULAlizer nevezetű program, amely éppen ezt feladatot szeretné a felhasználók számára megkönnyíteni. Kikeresi a kényes, kritikus részeket és ezek átolvasásával gyorsabban átrághatjuk magunkat rajta. A végén pedig eldönthetjük, egyetértünk-e vele, és elfogadjuk, vagy számunkra vállalhatatlanok a feltételek és akkor elállhatunk a beleegyezéstől.

5. fejezet: E-mailezés, jelszavak

Kulcsszavak: jelszóválasztás, jelmondat, egyedi jelszó, spam, spamszűrés, kéttényezős hitelesítés, https, lakat, SSL

Tények: Egy 2015-ös vírusvédelmi összefoglalóból az derült ki, hogy bár sokan ismerik az online világ veszélyeit, ám nem tesznek ellene megfelelő lépéseket. A megkérdezettek 82%-a aggódik a kiberbűnözés miatt, mégis például 62%-uk gyenge és rossz jelszavakat használ.

A 2015-ös Ashley-Madison incidensben, melynél a támadók 37 millió házasságtörő "ügyfél" adatát, benne neveket, e-mailcímeket, bankkártya számokat, szexuális preferenciákat, a tagság által feltöltött fotókat, illetve az ügyfelek és a belső munkatársak levelezését is megszerezték, az derült ki, hogy sokan a munkahelyi e-mail címükről regisztráltak. Az ott használt 11 millió jelszó visszafejtése után pedig az derült ki, hogy csak 4.6 millió volt egyedi, a többi rövid, gyenge és könnyen feltörhető volt. A "123456"-at 120 ezren választották, a "12345"-nak 48 ezer előfordulása volt, maga a "password" 39 ezerszer fordult elő.

Mit kell tudni az e-mailekről? Ez egy Nev@valami.hu formájú cím, amellyel levelezni tudunk. A jelszó olyan, mint a fogkefe: mindenkinek van, senkinek nem adjuk kölcsön és néha lecseréljük ugyanolyan fontos, mint a lakáskulcsunk: titkokat őriz, intim szféránkat védelmezi másoktól.

Milyen egy "jó" jelszó? Megjegyezhető, hosszú, legalább 10-15 karakter. Ne legyen szótári szó, ne adjuk oda másnak, és időnként akkor is cseréljük le, ha semmi baj nem történt. A jelszó ne legyen családtag, kutya neve, vagy szimpla születési dátum, és semmiképpen ne használjuk több helyen! Az is fontos, hogy a jelszó emlékeztető ne maga a jelszavunk legyen! Az olyan jelszó menedzserek, mint a LastPass, KeePass, segíthetnek a megjegyzésben. Ha valóban nagyon erős, „feltörhetetlen” jelszót szeretnénk választani, akkoriban jelszó helyett használhatunk jelmondatot, például "Imádom a forró csokoládét keksszel!" Ez már önmagában is hosszabb a korábbi szimpla szavaknál, ám ráadásul a mondatban szereplő szavakat még meg is bolondíthatjuk benne különféle trükkökkel, tovább nehezítve a visszafejtést. Kihagyhatunk belőle magán- vagy mássalhangzókat („hajókirándulás Szegedre” -> „hakindásgere”), játszhatunk a kezdőbetűkkel („Minden este hétkor vacsorázom, 8-kor fekszem le” -> „Me7v8fl&”), vagy a LEET átírásban (4 = A, 8 = B, 1 = L, , 3 = E, 7 = T, stb.) szereplő helyettesítésekkel is továbbkeverhetjük.

A jó jelszó fontossága mellett arról is érdemes szót ejteni, hogy milyenek a rossz jelszavak. Minden évben kiadásra kerül az úgynevezett „Worst Password List”, amely az adott esztendő legrosszabb jelszavak évi listája. Ebben sajnos évről évre az olyan rövid, gyenge, vagyis könnyen kitalálható vagy percek alatt egyszerűen feltörhető (brute force, szótár) szavak szerepelnek, amelyeket ráadásul sokszor több különböző belépési helyszínen is használ a gazdájuk. Ilyen elrettentő jelszavak például az abc, 123456, password, iloveyou,

abc123, stb.

A jelszóhosszal kapcsolatban érdemes megemlíteni azt az adatot, amely Dinya Péter szakdolgozatában szerepelt a visszafejtési idők hossza szerint. Ebben az látható, hogy a percek, órák, napok éppen a 10 karakteres hossz felett, 11 hosszától felfelé váltanak nagyságrendet, és lesz években mérhető a feltörés a mai hardverek számítási teljesítményét figyelembe véve .

Érdemes emellett még további óvintézkedéseket is foganatosítani. Használjunk több különböző email címet, legyen külön a játékhoz, és külön a barátokhoz, illetve a munkához. Ha egy alkalmi regisztráció miatt szükséges, használjunk eldobható e-mail címet! Az e-mail cím ne a teljes nevünk és születési évünk legyen, hiszen egy „kovacs.peter.1974@freemail.hu” cím túlságosan árulkodó. H kell, akkor a gyermek eleinte inkább kérjen segítséget, ha egy játék regisztrációhoz e-mail címre volna szüksége.

SSL - TLS:

A netes bankok, Google, PayPal, Yahoo, Facebook, Twitter, Steam, Dropbox, LinkedIn, Apple ID, Snapchat és többek közt a Reddit is úgy döntött, csatlakozik ebbe a klubba, és biztosítja a https kapcsolaton (SSL) keresztüli biztonságos bejelentkezést. Ekkor a név és jelszó adat nem sima, olvasható szöveggént, hanem titkosítva utazik a neten.

További jótanácsok a belépéseknél, hogy ahol lehetséges, használjuk a két faktoros azonosítást. A más néven a klasszikus, teljes értékű kétfaktoros hitelesítés eredetileg fizikailag is két különböző készüléket jelent, az egyiken - például PC-n - végezzük a bejelentkezést jelszóval, a másikon - például okostelefon - pedig ezenfelül minden egyes alkalommal kapunk egy tranzakciónként teljesen egyedi SMS kódot, és csak ezek együttes birtokában tudunk biztonságosan bejelentkezni, vagy tranzakciót indítani. Vagyis a jelszó ellopása vagy kitalálása mellett ilyenkor még a telefonunkat is el kellene lopnia a támadónak, ami azért jóval ritkábban sikerül.

Természetesen ha valaki mobilról bankol, akkor a klasszikus, teljes értékű kétfaktoros hitelesítés biztonsága csorbul, mert az eredetileg fizikailag is két különböző készüléket jelent, magyarul a számítógépes jelszavunk eltulajdonítása mellett a telefonunkat is el kellene lopnia a támadóknak.

A LinkedIn esetében biztosan sokan emlékeznek még a 2012-es incidensre, ahol 6.5 millió jelszó került illetéktelen kezekbe, mert az üzemeltetők nem támaszkodtak olyan megbízható kiegészítő technikákra, mint például a Salted hash, megnövelve ezáltal a jelszó hash hosszát, és egyúttal a bonyolultságát is. Ez is nagyban közrejátszott aztán abban, hogy a jobb későn, mint soha jegyében 2014. szeptemberében végre megvalósítsanak egy sor olyan biztonsági elemet és szolgáltatást, amelyek segíthetnek az ilyen helyzetek elkerülésében. Így az újragondolt LinkedIn alatt többek közt bevezetésre került az úgynevezett bejelentkezéssel kapcsolatos kontroll, amelynek segítségével könnyen ellenőrizhető, nem vagyunk-e éppen egy időben máshonnan is bejelentkezve, ha igen, akkor távolról ki lehet léptetni. Természetesen bevezetésre került a két faktoros

autentikáció, és emellett a jelszóváltoztatásról is egy külön e-mailes emlékeztető értesítést lehet kérni, ki mikor, milyen böngésző, milyen operációs rendszer alól, milyen IP címről és földrajzilag nagyjából honnan kezdeményezte mindezt.

A Google, PayPal, Yahoo, Facebook, Twitter, LinkedIn és Apple ID után 2015-ben végre a Reddit és a Snapchat is úgy döntött, eljött az ideje a biztonságosabb beléptetésnek. A Snapchat esetében a 9.9.0 verziójától kezdve lett választható a kéttényezős hitelesítés, amely itt is biztonságosabbá teheti a belépést. Minden olyan helyszínen, ahol erre mód van, érdemes használni és kihasználni a lehetőséget, és remélhetőleg sok felhasználó választja majd ezt mind iOS, minden pedig Android alatt. A Gmail és Apple iCloud esetén például kaphatunk értesítést, ha valaki illetéktelenül megpróbálna belépni a fiókunkba, vagy a nevünkben jelszót változtatna, erről e-mailben vagy SMS-ben is értesülhetünk.

Emlékeztet, hogy korábban nem kerülték el az adatszivárgási incidensek a Snapchat rendszerét sem, például a 4Chan-es történetben kiszivárgott meztelen celeb képek közül több ezret átküldtek a Snapchat üzenet rendszerén is, amelyek persze nem tűntek el nyomtalanul. De itt lehet megemlíteni például a Sapsave Android alkalmazást és a hasonlókat, melyek segítségével az elvileg tíz másodperces korlátozást megkerülve gyakorlatilag bármit le lehetett menteni. Emlékezzünk, azok a képek vannak a legnagyobb biztonságban, amelyet nem töltünk fel sehova.

Miért használtunk jelszavakat régen, és miért használunk ma?

Jelszava régebben jobbra a titkos társaságoknak, katonáknak volt. Emlékezzünk, hogy a Pál utcai grundra is a palánk ajtaján való négy egymásutáni szabályos koppantás azonosította, nem idegen érkezik. De ugyanígy kérdezte a sötét folyosón a szolgálattevő testőr tiszt is: "Állj, mi a mai jelszó?" És a továbbmenetelhez tudni kellett, hogy "Jupiter." A mesebeli Ali baba is a "Szezám tárulj fel" jelszóval tudott bejutni a sziklafal túskebokor mögötti ajtaján. A korai egyszerűbb titkosítások között is voltak olyanok, amelyeknél csak egy előre meghatározott jelszó birtokában a jogosultak számára lett érthető az idegeneknek zavarosnak látszó üzenet.

A jelenre nézve azonban már szinte nincs is, akinek az élete mentes lenne a különféle jelszavak kitalálása, megjegyzése alól. Ha lakótelepen lakunk, kapunk egy általában fix kapukódot, amivel igazolhatjuk a jogosultságot, magyarul azzal nyithatjuk ki. Ha mobil telefonunk van, a hangpostafiókunkhoz jár egy alapértelmezett jelszó. Ha internetszolgáltatóhoz tartozunk, illetve elektronikus postafiókunkba akarunk belépni, ezekhez is mind egy választott jelszó birtokában férhetünk hozzá. Ezeken felül a munkahelyünkön is további csoport munka, városi telefonhíváshoz tartozó kód, egyéni és hálózati login adatok, stb. társulnak. Ha ezekhez minden egyedi különböző, erős és nehezen kitalálható, valamint rendszeresen cserélt jelszót választunk, amikre később emlékezni is akarunk, alaposan felköthetjük a felkötendőt. A jelszavak ma már minden hétköznapi embert érintenek.

Éljen és virágozzon az alapértelmezett jelszó

Sokféle hibát követhet el egy átlagfelhasználó: operációs rendszerébe könnyen kitalálható - ergo törési eszközök alapszótárában szereplő - jelszót választ, a wifi routerhez nem állít be semmilyen titkosítást, vagy csak WEP-et, stb. Sokan csak elhozzák a boltból WiFi routert, kicsomagolják, és az adminisztrációs jelszót sem változtatják meg azonnal, aztán csodálkoznak, illetve ami még talán rosszabb, észre sem veszik a következményeket. Routers esetében mindig érdemes azonnal új adminisztrációs jelszót választani - ne a szomszéd, vagy egy utcáról netező zárjon ki minket a saját hálózatunkból, valamint a titkosítást is érdemes a viszonylag erős WPA2-re beállítani.

A fantáziátlanság csimborasszója

Nem tudni, hogy a kereskedelmi TV csatornák műsorszínvonalra hozta-e az áttörést, vagy egyéb behatások is felelősek a szürkeállomány ipari méretű leépüléséért, mindenesetre a jelszóválasztási fantáziátlanság az emberek többségénél világszerte katasztrofális. Az Errata Security 2009-es vizsgálata alapján, amely több ezer, PhpBB felhasználó jelszava alapján történt, az alábbi képet festi elénk, következzen hát a siralmas, mítoszromboló valóság. Nem a fórumjelszavak kinyerésének módjára gondoltunk, hanem a "talált" jelszavak minőségére. Először is a nyertesek: az "123456" és a "password" volt a leggyakoribb választott jelszó. De a Top10-es lista további elemei sem jobbak: ".phpbb", "qwerty", "12345", "12345678", "letmein", "1234", "test", "123". Pedig hát egy jól kitalált karaktersorozat ingyen van, és nem "letudni" vagy "kipipálni" való nyűgnek, hanem adatainkat védő, minket szolgáló eszköznek kellene felfogni a jelszóválasztási procedúrát. Korábban már szóba került ez a Conficker féreg kapcsán, hiszen ott is a támadás egyik módszere éppen a hálózati gyenge jelszavak elleni szótáralapú támadás.

A telefon okos, a felhasználó kevésbé

Egy ausztrál fiatalember visszaélve a jailbreakelt telefonokat használók tudatlanságával és/vagy lustaságával, az alapértelmezett SSH jelszót felhasználva írt egy C nyelvű férget, amely távolról belépett mások telefonjába, lezárta az SSH portot és felmásolt néhány állományt, többek közt lecserélte az iPhone háttérképet Rick Astley-re a tulajdonosoknál. Kíváncsi volt, vajon hány ilyen sebezhető készüléket talál, és állítólag száz fölötti darabszámba lelt így rá. A 21 esztendőes Ashley Towns úgy gondolta, csak egy ártalmatlan tréfa, amit tesz. Mondjuk úgy tűnik, valóban nem akart kárt okozni, és a feltűnően lecserélt háttérkép is ez látszik igazolni. Csak azok a feltört telefonok voltak ilyen veszélyben, amiken fut ez az említett SSH démon.

Sokan próbálnak különböző okok miatt a korlátozásoktól megszabadulni (függetlenítés=bármely telefonszolgáltatónál lehet használni a készüléket; jailbreak=tetszőleges, ingyenes, vagy feltört programok telepítési lehetősége a különben egyedüli fizetős iTunes helyett) és az ilyen esetek nyilván média értékűek az Apple-nek, hogy lám-lám, így jár aki nem az egyenes utat választja. Ráadásul ennek a támadásnak a C programja nyilvánosságra is került, ezért várhatóan további kevésbé barátságos verziók is megjelenhetnek majd. A védekezés egyébként egyszerű, nem más, mint egyedi SSH jelszó beállítása.

Gyógymódok gyanú esetére

Az incidens jeleinek észlelése szintén sokaknak problémát okoz. Pedig nincs rosszabb

forгатókönyv annál, mintha valakinek feltörіk és ellopják az accountját, de azt hosszú ideig vagy egyáltalán nem is veszi észre. De már a 2008-as Sarah Palin esetről is látszott, nem szükséges a Yahoo-t vagy a Gmailt feltörni ahhoz, hogy valakinek a postafiókjába mégis be lehessen jutni. De legyen bármi is a módszer, mit tegyen az, aki gyanítja, vagy éppen biztos benne, hogy a levelezését feltörték? A biztonsághoz való megfelelő hozzáállás az, hogy biztos információ nélkül, már pusztán gyanú esetén is úgy járjunk el, mintha biztosak lennénk a kompromittálásban. Az okok keresésében és a teendők megválasztásában az alábbiak talán segíthetnek.

- az érintett szolgáltató azonnali értesítése (pl. Gmailnél Google) az incidensről. Később az ő rendszer naplói segíthetnek majd a tisztázásban, felderítésben is. Ilyen esetekben a szolgáltatók igyekeznek mindent megtenni, és segítőkészek.

- használtam-e másik postafióknál, webes szolgáltatásban ugyanazt a jelszót? Mert ha igen, gyakori forgatókönyv, hogy egy jelszó megszerzésekor végigpróbálgatják az illető egyéb levelező, csevegő, webes, FTP eléréseit - és gyakran nem eredmény nélkül. Ha igen a válasz, akkor a feltört helyszínen mindenképpen, és az esetleges megegyező jelszavú helyeken úgyszintén azonnali jelszó csere szükséges.

- használtam-e túlságosan beszédes, könnyen kitalálható jelszó emlékeztető kérdést? Ha igen akkor azonnal meg kell változtatni. Ha esetleg ezzel egyező jelszó emlékeztető kérdés van másik helyszínen, akkor azonnal azt is változtatni. Ugyancsak a Sarah Palin email fiók feltörési esetről látszott, nem célszerű ész nélkül minden személyes adatot túlzottan kiakasztani a közösségi oldalakra. Mi is volt ott a probléma? A módszer nem feltörés, nem jelszó találgatás volt, hanem új jelszó igénylése. A születési hely és idő megszerzése nem okozott gondot, a titkos ellenőrző kérdés pedig az volt, hol ismerkedtek meg a férjével. Az ismert és kevésbé ismert embereknek komolyan el kellene gondolkodniuk, érdemes-e olyan adattal védeni bármit is, amit a bulvárlapok lapok hetente megírnak, vagy valaki önként kiakasztja az IWIW-es lapjára.

- Használtam-e a jelszavamat nyilvános helyen: kávézóban, hotspoton, kileszette-e valaki a vállam felett? Találtam-e a kocsim mellett (direkt-véletlenül nekem csalinak odahelyezett) USB kulcsot, vagy egyéb eszközt, amit a gépembe később bedugtam? Ha bármelyik kérdésre igen a válasz, érdemes a jövőben ezekre kiemelten figyelni.

- Adatvagyon leltár felmérése. Milyen bizalmas adatok voltak a levelezésben, amik ha illetéktelen kezekbe kerültek, bajt okozhatnak? További szolgáltatásokhoz, munkahelyi elérések belépő jelszavai, partnereinkkel folytatott levelezések, magánéleti dolgok, amiket nem szívesen látnánk a subba blogon vagy a szanalmas.hu oldalakon. Teendő lehet a levelekben szereplő összes account haladéktalan megváltoztatása, fontosabb üzleti partnerek figyelmeztetése, ismerőseink, rokonaink, barátaink értesítése, hogy postafiókunk áldozatul esett, és ha x-től - y időtartamig a nevünkben levelet kaptak, ellenőrizték le annak tartalmát velünk külön egyeztetve. 2010 márciusában ismeretlen elkövetők például a tulajdonos Propeller.hu nevében beadtak egy törlési kérelmet is a Google-hoz.

- Ha bankkártya számok, elektronikus fizetés adatok is szerepeltek, akkor a banki egyenleg, tranzakciók azonnali vizsgálata a kétes időszakra. Ugyanez vonatkozik a fizetős online játékokra is, például World of Warcraft, és hasonlók.

- Feljelentést tenni a rendőrségen az ügyben. Indokolt esetben mind a Google központjától, mint az érintett IP cím aktuális felhasználójának internetszolgáltatótól való kikérése megtörténhet a nyomozás folyamán.

- Beléptünk-e bármilyen webes levelezésbe, szolgáltatásba, és kipipáltuk-e az "Emlékezz rám" vagy a "Maradjak belépve" opciókat? Ha igen, üssünk a kezünkre és többet ne tegyünk ilyet;-)

- És érdemes lehet egy alapos vírus és kémprogram ellenőrzést is tartani a biztonság kedvéért.

- Végül imádkozni, hogy ne legyenek további kellemetlenségek, és megfogadni szent esküvással az erős jelszó használatát, mindenhol másikat alkalmazni, és ezeket rendszeres időközönként cserélni, valamint Facebook, AppleID, Google, stb. profilunk átgondolását a jelszó emlékeztető kérdésekkel kapcsolatban, fokozott óvatossággal viselkedni a jövőben.

Sajnos gyerekek és felnőttek között is előfordul, hogy megtudva a másik fél jelszavát, ezzel visszaélve titokban beleolvasnak a másik levelezésébe, vagy durvább esetben a másik fél nevében üzeneteket írnak, kimerítve ezzel a levél- és magántitok megsértését, a személyes adattal való visszaélést, vagy akár a becsületsértést.

Összefoglalva: a jelszóval való törődés nem azért van, hogy bosszantson minket, hanem hogy sikerrel szolgáljon, védjen bennünket, amit meg is tesz, ha mi is gondosan állunk hozzá. Ha rendszeresen cseréljük, kellően erőset választunk és nem ugyanazt használjuk mindenhol, máris sokat tettünk – saját magunkért. Persze igaz, ezek az erőfeszítések, jelszócserek munkát, folyamatos törődést és odafigyelést igényelnek, de akárcsak a biztonsági mentések készítésénél, itt is megtérül a befektetés, ha legyőzzük a lustaságunkat.

Egy 2014-es kutatás szerint a korábbi IT dolgozók jelszava sok helyen még hosszú hónapokkal, sőt évekkel később is élő marad, mivel azt nem kapcsolták le - nem hogy azonnal az épületből való távozáskor, de még azóta sem. A HelpNetSecurity jelentése szerint a korábbi számítástechnikai munkavállalók negyede azóta is régi jelszavával hozzáfér volt munkahelye hálózatához. Sőt hogy még elképesztőbb legyen a kép, 16% egyenesen úgy nyilatkozott, nem csak egy, hanem összes korábbi munkahelyi környezetéhez megvan még az élő hozzáférése. Ha ehhez pedig hozzávesszük mondjuk a Verizonnak azt a kimutatását, miszerint a komolyabb fajsúlyú adatsértések, incidensek rendre gyenge vagy eltulajdonított belépési adatok miatt következnek be, akkor jól látható, mekkora vétkes mulasztás is mindez az IT részéről.

A levelezés illemszabályairól is rendezik az úgynevezett Netikett, érdemes ezeket is beidézni:

„Ne írd semmi olyasmit egy elektronikus levélbe, amit nem küldenél el levelezőlapon.

Ha továbbküldesz (forward) vagy újrastárolsz egy üzenetet, akkor ne változtasd meg annak a szóhasználatát. Ha ez egy neked írt személyes üzenet volt, és egy csoportnak kívánod továbbadni, akkor kérjél először engedélyt a feladótól.

Soha ne küldj "lánc" levelet elektronikusan, ezek tiltottak az Interneten.

Egy jó ökölszabály: légy konzervatív a küldésben és légy liberális a fogadásban. Nem szabad indulatos leveleket küldened (ezeket "flame"-nek nevezzük) még akkor sem, ha provokálnak. Másik oldalról viszont, ne legyél meglepve, ha ilyen levelet kapsz, és okosan teszed, ha nem válaszolsz ezekre.

Figyeld a cc:-kre a válaszoláskor. Amikor már csak két ember között folyik a kommunikáció, akkor ne küldd el ezeket a leveleket másoknak.

Használj vegyesen kis- és nagybetűt, akárcsak a közönséges íráskor. A CSUPA NAGYBETŰ OLYAN, MINTHA ORDÍTANÁL!

Használj "mosolygókat" (smiley) a hangszín jelzésére, de bánj velünk takarékosan. :-) példa ilyen "mosolygóra" (dönts oldalra a fejed és nézd meg úgy.) Azonban ne feltételezd, hogy egy "mosolygó" szerepeltetése rögtön eléri, hogy a címzett egyetértsen veled, vagy hogy egy egyébként bántó megjegyzés élet elvegye.

Légy tömör anélkül, hogy túlságosan lényegre törő lennél. Amikor egy levélre válaszolsz, csak annyit idézz az eredeti anyagból, hogy érthető legyen a válaszod és ne többet. Rendkívül rossz szokás az egész levelet idézni a válaszban - töröld ki a felesleget.

A levél fejlécében kell, hogy legyen egy subject sor, ami visszatükrözi a levél tartalmát.

Küldj egy rövid választ a feladónak, hogy megkaptad a levelét, ha úgy gondolsz, hogy a levél fontossága szükségessé teszi ezt. Tedd meg ezt akkor is, ha részletesen válaszolni csak később lesz idő.

Ne küldj nagy tömegű kéretlen információt az embereknek. „

6. fejezet: Közösségi oldalak, digitális lábnyom

Kulcsszavak: instant azonnali érzelmi szükség kielégítés, megosztás, az internet nem felejt

Tények: Több millió Facebook felhasználó van, aki nem (csak) számítógépről lép be a felületre, de emellett a mobil felhasználás a Facebook hirdetési bevételeinek 30%-át generálja. A közösségi média egyébként már egy ideje megelőzte a pornográfiát, többen űzik ezt az interneten elsődleges tevékenységként.

A Webroot egy átfogó felmérés keretében mintegy ezeregyszáz Facebook-, MySpace-, Twitter-, Linkedlin-felhasználót kérdezett ki a webhasználati szokásairól. Az eredmények alapján elmondhatjuk, az óvatosság sajnos nem igazán jellemző. A válaszadók kétharmada egyáltalán nem korlátozza a személyes profiljában olvasható részleteket, amelyek így akár egy Google keresővel is láthatóak. Több mint a felük (59%) nem tudja biztosan, kiknek is engedélyezte pontosan profilja megtekintését. Körülbelül egyharmaduk (32%) adott meg legalább három személyes azonosításra alkalmas információt, egyharmaduk (36%) ugyanazt a közösségi portálon használt jelszavát máshol is használja, egynegyedük (28%) fogad el barátkérőt idegentől. Más mutatók sem festenek szebb képet. Az igaz, hogy 78% aggódik személyes adatai miatt, de ugyanakkor 30% nem rendelkezik vírus- és kémprogram elleni védelemmel. A korosztályok közt a fiatalok számítanak a legveszélyeztetettebbnek, az átlagos 28 százalékos értékkel szemben náluk 40 százalék fogad el barátkérőt idegentől, és náluk sokkal jellemzőbb az összes személyes adat, elérhetőség megadása is.

A Nominet nevű internetes cég egy 2015-ös tanulmányából az derült ki, hogy az Egyesült Királyságban a szülők átlagosan mintegy 200 fényképet töltenek fel minden évben az 5 évesnél fiatalabb korú gyermekükről, aki csak felnőve fog majd szembesülni ezzel a közel 1000 fotóval. Eközben Franciaországban szigorúak a rendelkezések, hiszen akár egy év börtönbüntetést is kaphatnak azok a szülők, akik gyerekeiket ábrázoló fotót posztolnak. A képmáshoz fűződő jogszabályok ugyanis a kiskorú, cselekvőképtelen gyermekeket ábrázoló fényképek felelőtlen szülői engedély nélküli képmegosztásáért elzárással, vagy 45 ezer EUR összeggel is szankcionálhatják.

Facebook - Közösségi hálózatok

- Látszólag senki nem tartja be a 13 éves korhatárt. Igaz, sokszor már az iskolákon belül is itt zajlik a kommunikációt, a tanár ide az osztály zárt csoportjába írja, hogy másnap mindenki hozzon körzött. Az is megfigyelhető, hogy a tinik igyekeznek máshova menni, mint ahol a szülei is fent vannak, nekik a Facebook emiatt már ciki. Van is hova menniük, hiszen számtalan alternatíva létezik, például YouTube, Twitter, Google Plus, Instagram, Snapchat, Reddit, Tumblr, Pinterest, Vine és LinkedIn. De ezen felül is egy csomó helyre mehetnek még Facebook helyett: chatroulette, Tinder, ask.fm, sőt az is előfordult, hogy egy alig látogatott Utah-i ingatlanközvetítő fórumát fedezték fel maguknak, ahol regisztráció nélkül lehetett írni, beszélgetni. A Chatroulette oldalt - amelyen véletlenszerűen sorsol össze a gép egy másik felhasználóval - egyenesen a net szexuális ragadozóinak paradicsomaként emlegetik. Igaz, névleg legalább 16 évesnek kell/kellene

lenni a regisztrációhoz, azonban kiskorúként, de nagykorúként is az idegenekkel való webkamerás kapcsolat rengeteg veszélyt rejt, érdemes ezzel minden szülőnek tisztában lennie. Egyébként a Tinder később átgondolta a dolgot, és 2016. júniustól a korábbi 13 éves korhatárról 18-ra emelte a regisztráláskori engedélyezett életkort. Bár a működésben így is egymás közt, azaz a 13-17 közöttieket ajánlották a kiskorúaknak, és nem felnőtteket, most a felelősségteljeség jegyében szigorítanak. Ez azonban sajnos nem gátja annak, hogy a Facebookhoz hasonlóan továbbra is hamis életkori megjelöléssel regisztráljanak a kiskorúak.

Bár az egyes közösségi oldalak tesznek kisebb lépéseket a tartalmak kordában tartására, ez korántsem elegendő. Például az Instagram tartalmaz egy úgynevezett tiltott kulcsszavak (banned hashtags) listáját, amelyen igyekeznek a legdurvább kategóriákat távol tartani a képmegosztótól.

„A magánélet a múlt társadalmi normája. A személyiség jogainak védelme felett eljárt az idő” - véli Mark Zuckerberg. Az emberek egy része, különösen az IT biztonsággal foglalkozó szakemberek, a felhasználók biztonságtudatos csoportjának azonban inkább negatív erről a véleménye. Mindent részletesen megosztani az életünkből körülbelül annyi értelme van, mint atombunkert építeni Kocsordon. Nem véletlen az sem, hogy az antivírus blognak nincs rajongói Facebook klubja sem, hiszen ezekről rendre lebeszélünk mindenkit. Nem tévedünk sokat, ha úgy gondoljuk, sokan fogják megbánni később, hogy meggondolatlan üzeneteikben felelőtlenül kitárulkoztak, munkahelyüket, karrierjüket, barátaikat, családjukat szidalmazták. Nem egyszerű hát minden szempontot, összefüggést és ehhez az adatvédelem módjait saját életünkben kiépíteni, megőrizni, és ha valamire áll, akkor erre igazán: ez egy élethosszig tartó tanulási folyamat.

Ideje leszámolni az "Én egy egyszerű hétköznapi ember vagyok, ugyan mit tudnának nekem ártani a számítógépes bűnözők" című téveszmével. Meglepő módon azt is mondhatjuk, csatlakozni egy Facebook csoporthoz kockázatosabb, mint egy direkt linken érkező kártevőre kattintani. De miért-e nagy maliciózus kijelentés? Íme példaként egy olyan Facebookos csoport, amelyik eredetileg magasztos és pozitív célok érdekében alakult: a Haiti földrengés áldozatainak gyűjtöttek adományokat. Csalók azonban megváltoztatták csoport nevét Svéd Nekrofilek Egyesületévé, sőt még egy üzenetet is kiírtak a csoport weboldalára: "Ahogy mindnyájan tudjátok, a Svéd Nekrofilek Egyesülete 500 ezer koronát adományoz arra a célra, hogy a Haitiról visszahozott holttestek minél jobb állapotban legyenek, hogy közösülhessünk velük". Egyáltalán nem vicces a dolog, és valószínűleg senkinek nem hiányzik, hogy a nevét leendő munkaadója egy ilyen tömörülésben találja meg. Egy érdekes felmérés szerint az amerikai személyzetisek 70%-a utasított már el állásra jelentkezőt amiatt, hogy negatív lett a közösségi oldaláról begyűjtött információ a jelöltről. Figyelemreméltó naivság, hogy ennek ellenére a leendő álláskeresőknak mindössze csak a 7%-a gondolja úgy, hogy ezek az adatok egyáltalán befolyásolhatják a pályázatukat.

Egy érdekes kommentből igen szemléletesen látszik az, hogy mennyire nincsenek az emberek tisztában azzal, hogy ami információt, képet, adatot megosztanak magukról, az

menyire árulkodó lehet mások számára. „Volt egy kolléganőm, aki állandóan a gyerekével büszkélkedett, szinte már hihetetlen dolgokat állítva. Mivel elég egyedi családnevük van, amikor még létezett, rákerestem az IWIW-en, meg is találtam a gyereket, közös fotó is volt fenn róla a kolléganőmmel. (A fotón rajta volt a házuk utcanevével és házszámmal, meg az autójuk rendszámmal.) Tovább keresgélve azt is megállapíthattam, hogy a srácnak angolból pótérettségire kellett mennie (mert az iskola kipakolja az internetre az erre vonatkozó exceltáblát!), valamint azt is megállapíthattam, hogy a gyerek egy huszadrangú gimibe jár, nem pedig abba az elitgimnáziumba, amit a kedves mamája állított. A huszadrangú gimnázium viszont nem csak a szégyeninfókat közli, hanem valamennyi osztályáról közös osztályképet tesz fel minden évben a netre, ezen is megtaláltam a srácot. Ennyire nincsenek tisztában az emberek (szülők, tanárok) azzal, hogy milyen következményei vannak a képek, adatok megosztásának."

A Pleaserobme.com honlap egészen érdekes dolgot mutat meg: nagyon sokan interurbán realtime közvetítésként osztják meg életünk minden apró rezdülését a nagyérdeművel: most fordulok be a sarkon most csekkoltam be ezen és ezen a reptéren, stb. Az általuk mellékelt keresési javaslattal élve magunk is meggyőződhetünk arról, hogy éppen ebben a pillanatban is milyen sokan közlik a pillanatnyi helyzetüket. Nem kell GPS vagy okostelefon póráz a munkaadónak, de a betörők is minden bizonnyal örülnek az ilyen nüanszokra kihegyezett részletes online közvetítésnek, mert ebből jól látszik, hogy lesz-e még idő kivinni a plazma Tv-t is a teherautóba. Pláne, ha még a "nyaralni mentünk Mallorcára, hurrá" kezdetű bejegyzést is olvasták.

Sokan esnek abba a hibába, hogy alábecsülik a szülők viselkedésének mintaadási funkcióját. Pedig óriási jelentősége van ennek. Ha például a gyerek rendetlenséget lát a szülő íróasztalán, lehet, hogy hiába kérleljük majd a játékpalc elpakolására. De ugyanígy érdemes – persze a saját korának megfelelően – válaszolni is a kérdéseire az egyszerű tiltások helyett, amelyek értetlenségre, „csak azért is”-típusú dakra vezethetnek. Meg kell értetni vele, miért nem tesszük közszemlére az összes személyes adatunkat, mik a veszélyei a bárki által nézegethető kihívó, fürdőruhás képeknek, milyen honlapoktól jobb, ha óvakodik, miért nem plakátoljuk ki, mikor utazik el a család nyaralni stb. Persze ez a nehezebb út, sok türelmet igényel, de hosszú távon mindenképpen célravezetőbb.

Ha felnőtt fejjel mindezt már belátjuk, akkor jön a család, a gyerekek kérdése. Sokan esnek abba a hibába, hogy alábecsülik a szülők viselkedésének mintaadási funkcióját. Pedig óriási jelentősége van ennek. Ha például a gyerek rendetlenséget lát a szülő íróasztalán, lehet, hogy hiába kérleljük majd a játékpalc elpakolására. De ugyanígy érdemes – persze a saját korának megfelelően – válaszolni is a kérdéseire az egyszerű tiltások helyett, amelyek értetlenségre, „csak azért is”-típusú dakra vezethetnek. Meg kell értetni vele, miért nem tesszük közszemlére az összes személyes adatunkat, mik a veszélyei a bárki által nézegethető kihívó, fürdőruhás képeknek, milyen honlapoktól jobb, ha óvakodik, miért nem plakátoljuk ki, mikor utazik el a család nyaralni stb. Persze ez a nehezebb út, sok türelmet igényel, de hosszú távon mindenképpen célravezetőbb. Tudniuk kell azt is, hogy nem mindenki az, akinek látszik. A közösségi oldalakon is vannak olyan rejtőzködő bűnözők, pedofilok, akik adatlapjuk alapján látszólag gyerekek, de

valójában az a céljuk, hogy kikérdezzék, és behálózzák a gyanútlanabbakat, akár az elkotyogott információkkal történő zsarolással. Sose adják meg minden személyes adatukat a közösségi portálokon, mert mások visszaélhetnek vele! Csak ha már valóban ismerősünk valaki, elég akkor odaadni a telefonszámunkat, lakcímünket vagy e-mail címünket. Bár sok felnőtt is elköveti ezt a hibát, de a gyermekek esetében ez sokkal veszélyesebb, ráadásul ők hajlamosak naivan mindent elárulni, ezért kiemelten a szülő feladata, hogy megbeszélje a gyerekkel ezen dolgot, illetve tanácsot adjon. Tanulságos történet lehet az is, amikor a MI6 brit titkosszolgálat főnökének felesége óvatlanul még a lakcímét is közzéteszi a Facebookon. Egy felelőtlen családtag nagyon gyenge láncszem lehet. Egy amerikai felmérés szerint a 12 évesnél idősebb gyerekeknek már a fele (48%) tagja a közösségi portáloknak, és azt naponta többször is használja. Ez az a korosztály, akik szerint az e-mail már lassú és körülményes. Az újság és a televízió helyett is jelentős mértékben támaszkodnak inkább ezekre a pörgő, hihetetlen tempóban növekvő, és villámgyors web2 lehetőségekre.

Tudniuk kell azt is, hogy nem mindenki az, akinek látszik. A közösségi oldalakon is vannak olyan rejtőzködő bűnözők, pedofilok, akik adatlapjuk alapján látszólag gyerekek, de valójában az a céljuk, hogy kikérdezzék, és behálózzák a gyanútlanabbakat, akár az elkotyogott információkkal történő zsarolással. Sose adjuk meg minden személyes adatukat a közösségi portálokon, mert mások visszaélhetnek vele! Csak ha már valóban ismerősünk valaki, elég akkor odaadni a telefonszámunkat, lakcímünket vagy e-mail címünket.

A Facebook Graph Search segítségével pedig tetszőleges kifejezés, szokás, tulajdonság alapján tudunk keresni, és ebből az is látszik, ki milyen fényképeket, posztokat, vagy kommenteket kedvelt, lájkolt. Ez igazi „lábnyom” rólunk.

Egy felelőtlen családtag nagyon gyenge láncszem lehet. Sok felnőtt is elköveti ezt a hibát, tanulságos történet volt például az is, amikor 2009-ben az MI6 brit titkosszolgálat főnökének felesége óvatlanul magas rangú vendégekkel közös nyaralási fotóit, de még saját a lakcímüket is közzétette a Facebookon - a férj leváltása lett a vége. De a gyermekek esetében ez még sokkal veszélyesebb, ráadásul ők hajlamosak naivan mindent elárulni, ezért kiemelten fontos a szülő feladata, hogy megbeszélje a gyerekkel ezen dolgot, illetve tanácsot adjon, mit oszthat meg és mit nem. De az is fontos figyelmeztetés lehet, hogy egy 2011-ben elvégzett felmérés szerint, amelyet brit börtönökben végeztek el az derült ki, hogy a betörők csaknem 80 százaléka aktívan használja a Twitter, Facebook, Google StreetView és egyéb közösségi oldalak adatait a bűncselekményeire való felkészülésnél.

Muszáj megtanulni, hogy fontos az óvatosság: nem jelentjük be előre, hogy nyaralni indulunk, nem töltünk fel képeket magunkról meztelenül, nem töltünk fel képeket senkiről az ő beleegyezése nélkül, nem töltünk fel képeket a lakásunk belsejéről, értéktárgyainkról. Időnként érdemes átvizsgálni a biztonsági beállításainkat, ugyanis gyakori a változtatás a szolgáltatók részéről, például automatikusan megengedőbbre, közlékenyebbre állítódik át. Gyermekek esetén hasznos lehet a tanács, hogy ne legyen nyilvános a profiljuk. Plusz segítség, hogy zaklatás esetén létezik a „jelentem” gomb.

A Facebook a maga módján igyekszik valamennyit segíteni. Ha valaki a valós életkorával regisztrál, akkor a 13-18 életév között szigorúbbak az alapbeállítások, például alaphelyzetben nem publikusak a posztok, és nem publikus a profil. Emellett létezik a már emlegetett „jelentem” gomb, valamint az Interpollal is jó kapcsolatban vannak, így a visszaélések - például pedofília - esetében igen gyorsan tudnak lépni a gyermekek érdekében.

Sajnos számos rossz szokás is jelen van a neten, amelyet főképp a nagyobb fiatalok jópofának, viccesnek tartanak. Az egyik ilyen például, hogy „#aftersex” címkével ellátott selfieket (önportrékat) töltenek fel a Facebook, Snapchat és Instagram oldalaira. Egy ezzel foglalkozó cikk szerint a szex utáni szelfik 2014-ben lepték el tömegesen Instagramot, így az „#aftersex selfie” hashtagre rákeresve már több, mint 60 000 ilyen címkével rendelkező fényképet lehet találni. A viccesnek szánt képaláírások között pedig rengeteg olyat lehet találni, mint például „ki ez itt mellettem?” vagy „valaki mentsen ki”.

Természetesen az emberi tényező ott van mindenhol. Most sem tart senki töltött pisztolyt senki fejéhez, hogy bizalmas adatait, képeit, magánvéleményét kontroll nélkül gépelje be és ossza meg a világgal. Valószínűleg a megváltoztatott biztonsági beállítások a felhasználók egy nagy részét így is hidegen hagyja majd: nem érdekli, lusta rá, nem is hallott róla, nem ért hozzá illetve fogalma sincs, hogy az ő személyes adatai is nyilvánosak. És ezzel a hozzáállással pontosan ők azok, akiknek adatai, képei, megnyilvánulásai egyszer majd valamilyen kínos helyen kötnek ki. Nem tévedünk sokat, ha úgy gondoljuk, sokan fogják megbánni később, hogy meggondolatlan képeikkel, üzeneteikkel felelőtlenül kitarulkoztak, vagy éppen iskolájukat, munkahelyüket, karrierjüket, barátait, családjukat szidalmazták.

Az adatok megosztásában, és a privacy miatti aggodalomban a fiatalok látszólag sokkal rugalmasabbak. Valójában azonban sokszor inkább csak naivak, tapasztalatlanok, gyakorta nem elég biztonságtudatosak. Ha elég időssek lesznek, és jobban megismerik a kockázatokat, valószínűleg jobban megértik majd, hogy az esetleg felelőtlenül megosztott adataik miatt esetleg nem kapnak hitelt, vagy nem kapnak meg egy állást.

A megosztás emellett oda-vissza is probléma lehet: a gyerek is kérdezzen a szülőtől, de a szülők se töltsenek fel eszetlenül, átgondolatlanul képeket publikusan a gyermekeikről. A Huffington Post egyik erről szóló cikkében azt írják, hogy minden ötödik szülő saját bevallása szerint is posztolt már olyan képet vagy bejegyzést, ami ciki volt vagy lehet a gyermekére nézve. 10%-kukkal pedig az is előfordult, hogy a gyerekük reklamált náluk, és arra kérte őket, hogy vegyék le az adott fotót. A megkérdezett szülőknek a 7 százaléka tett már valamiféle negatív vagy kritizáló megjegyzést a gyerekére online, jórészt annak viselkedése miatt.

Tartsd tiszteletben mások privát szféráját, ha más valaki is szerepel egy közös fényképen, akkor először kérdezd meg tőle, hozzájárul-e a feltöltéshez, megosztáshoz.

Instagramnál az „Add to photo map” opcióval érdemes óvatosan bánni, hiszen ilyenkor a fizikai koordinátáink is megismerhetők lesznek.

A közösségi oldalakon se hagyjuk őt egyedül

Itt oszlanak meg leginkább a vélemények, mi a helyes módszer. Lehetünk egy üres profillal figyelve a barátai között, de van ahol elég, ha időnként megbeszéljük a szülőkkel a problémás szituációkat. Szerencsére ebben vannak biztató jelek is, például a tinédzserek 41%-a kér tanácsot a szüleitől privát szférájának védelmére. Legyünk olyan szülők, akiktől érdemes kérdezni, és mi is tanuljunk folyamatosan, mik a tipikus problémák, mik lehetnek a megoldások.

Fontos megjegyezni, hogy mi magunk tehetünk a legtöbbet saját privát szféránk védelméért. Aki gondolkodás nélkül, felelőtlenül megoszt magáról mindent, tulajdonképpen önként jelenti fel magát, szolgáltat ehhez publikus muníciót. Veszélyei pedig igen is vannak, a statisztikák alapján például a betörők 80%-a aktívan használja Google Maps-et, és a közösségi oldalakat. Én nem értek egyet azzal, hogy életünk minden részletét meg kellene osztani másokkal, és közben egyúttal az adatgyűjtő cégekkel is. Ezzel a magatartással tulajdonképpen bután kihívjuk magunk ellen a sorsot, a következmények pedig, ha nem is azonnal, előbb-utóbb mindig megérkeznek. A Snowden által leleplezett titkok fényében világosan látható, a túl sok adat gyűjtése nem azért aggályos, mert csak a terrorista gyanús elemek ellen irányult, hanem mert kivétel nélkül mindenki megfigyelésével járt. Emellett abban sem lehetünk biztosak, hogy valójában nem örök időkre őrzik meg ezeket, ami valljuk be, félelmetes.

Jó lenne széles körben a biztonságtudatosságra, a tájékozottságon alapuló védekezésre fókuszálni, nevelni, lehetne mindig előbb gondolkodni, aztán cselekedni, és ehhez létezik is számos ökölszabály, említsünk egy párat. Ami egyszer felkerül a netre, örökre ott is marad. Nem osztjuk meg pillanatnyi fizikai helyzetünket még "ingyen" ajándékokért sem. Csak a leragasztott webkamera a jó kamera, sok incidens bizonyítja, mennyire hatékony kém eszköz ez. Összefoglalva, bár lehetnének okos viselkedési mintáink, sajnos elenyészően kevesen figyelnek oda erre. Például annak idején a szökésben lévő John McAfee is úgy bukott le, hogy egy Guatemalai üdülőhelyről képeket töltött fel a mobiljával, amelyben benne voltak a földrajzi metaadatok.

A csevegés illemszabályairól is rendezik az úgynevezett Netikett, érdemes ezeket is beidézni:

„Akárcsak más rendszereknél, itt is bölcs dolog csak figyelni egy kicsit, hogy a csoport kultúrájához szokhassál.

Egyáltalán nem szükséges mindenkit személyesen üdvözölni egy csatornán ill. szobában. Egy szimpla Hello vagy hasonló köszöntés bőven elég. NEM elfogadott viselkedés, ha a szoftvered automatikáját arra használod, hogy mindenkit üdvözöljön.

Figyelmeztess a résztvevőket ha nagyobb mennyiségű információt szeretnél velük

megosztani. Ha mindenki egyetért vele, akkor mehet. E nélkül azonban súlyos udvariatlanság ilyesmit csinálni - akárcsak levélben.

Ne tételezd fel, hogy ismeretlen emberek beszélni akarnak veled. Ha kényszerítve érzed magad arra, hogy személyes üzenetet küldjél egy ismeretlennek, akkor készülj fel arra, hogy éppen elfoglalt lehet vagy egészen egyszerűen nem akar veled beszélgetni.

Ha valaki becenevet, alias-t, pseudonevet vagy hasonlót használ, akkor tiszteld az anonimitáshoz való jogát. Még ha esetleg jó barátok is vagytok, akkor is udvariasabb ezt a becenevet használni. Egyáltalán ne használd a valódi nevét on-line engedély nélkül."

Király Linda himnusz, 2003. Kelet–Nyugat Kosárlabdagála

Az "ami egyszer felkerült a netre, azt onnan többet nem lehet letörölni", valamint hogy az utólagos töröltetés miért nem működik - sőt épp ellenkező hatást vált ki - erre a legjobb példa, esetre talán az egyik legtanulságosabb példa, ha megörökítik azt, amikor sajnálatos módon elfelejtjük a Himnusz szövegét. Amikor 2003-ban a Kelet-Nyugat Kosárlabda Gálán a Budapest Sportarénában Király Linda szerencsétlen módon csúfosan belesült a Himnusz éneklésbe, mert nem tudta annak a szövegét, és az ezt megörökítő kínos felvétel bejárta a videómegosztó oldalakat. Még évekkel később is sokszor kérdezték őt erről a különféle interjúkban. Megpróbálták eltüntetni a videót a netről, és ezzel kapcsolatban megfogalmazott egy hivatalos levelet is. "Egy régi, kilenc évvel ezelőtti előadásomból kiragadott részt használtak fel, hogy hiteltelenítsék éneklési képességeimet és tönkretegyék karrieremet" írta a panaszlevelében. 2014-ben aztán az apja olyan módon próbálta meg eltüntetni ezeket a videókat az internetről, hogy egy új ötlettel vezérelve megvásárolta és levédette az inkriminált felvétel szerzői jogát nem kevés pénzért, majd ügyvédei útján perrel fenyegette meg a különféle videó megosztó oldalakat, hogy azonnal távolítsák el el a videót. "Tisztelt XXX, Mi, a Crown Music Bt., mint az alábbi linken található videó 2014. február 4-től online felületeken történő felhasználásának egyedüli jogtulajdonosa, kérjük a videó azonnali eltávolítását az oldalukról. Amennyiben kérésünknek nem tesznek eleget, a hatályos jogszabályok alapján jogi útra fogjuk terelni az ügyet. Együttműködésükben bízva, Király Tamás, ügyvezető." Ez az eljárás nem lehetett olcsó, de látszólag hatott: az Indavideo, és a YouTube ezt azonnal meg is tette, azonban ezzel hosszú távon mégis pont ellentétes hatást értek el, mert a felfokozott érdeklődés miatt sokan ismét kíváncsiak lettek rá, és néhányan a felvételt olyan weboldalakra, mint a Kurucinfo, vagy már távoli egzotikus, szabályozatlan jogrendszerű országok videómegosztóira töltötték fel - mint Malajzia vagy Dél-Vietnam - ahol az Európában vagy Amerikában alkalmazott jogrendszer viszont már nem tehetett semmit. Az törlés hírére azonban százszor annyian kerestek rá a felvételre, és ezzel csak tovább gerjesztették a felvétel iránti kíváncsiságot. Zárásképpen azt is érdemes megjegyezni, ha valaki beírja a keresőbe a "Király Linda himnusz" szavakat, még ma is fog rá találatot kapni. Az internet nem felejt.

A közösségi oldalaknál is meg vannak a tipikus csalási, átverési formák. Például előre lájkolás, Mi az indián neved, Találd ki milyen állat lennél, Melyik celebre hasonlítasz, ingyen iPhone, stb.

Mire lehet használni ilyen személyes adatokat? Hát először is lehet szipkázni olyan infót, amivel jól válaszolhatunk a jelszó-émlékeztető kérdésekre. De új típusú csalások is terjedőben vannak, például a személyes lapról kinézett barátok nevében Facebook üzenetet írnak az áldozatnak, hogy állítólag elvesztették a reptéren a mobiljukat, útlevelüket. A feltört fiókok így jól felhasználhatóak csalásra. Látszólag az ismerős nevében lehet üzenetet küldeni a barátoknak: „Hello, Londonban vagyok, ellopták a pénztárcámat, tudnál nekem pénzt küldeni?” Több alváltozat is ismeretes, de a lényeg, gyorsan egy kevés pénz segítséget szeretnének kérni, általában a Western Unionon keresztül. Ha valaki pedig segítőkész és bedől, keresztet vethet az ilyen átutalt pénzre. És mindig lesz, aki küld. Nyilván nem lehet figyelmen kívül hagyni a magyar felhasználókat sem, körülbelül 1.3 millióan lehetnek, és egy részük beszél angolul, vannak külföldi barátaik, ismerőseik.

Néhány dolog, amire vigyázzunk a Facebookon - biztonsági útmutató

Az ezer leglátogatottabb oldal listáját a Facebook vezeti napi 936 millió látogatóval. A közösségnek pedig már több mint 1 milliárd 440 millió aktív felhasználója van. Átlagosan minden tagnak körülbelül 130 ismerőse van, a tagok pedig havonta mintegy egymilliárd képet töltenek fel. Emellett 70%-uk valamilyen alkalmazást, játékot is futtat az oldal kínálatából. Mindegyikük kapcsolódik 80 további oldalhoz, csoporthoz, rendezvényhez és minden hónapban körülbelül 90 új tartalmat - bejegyzés, üzenet, kép, videó - hoz létre.

A Facebook egy terep, ahogy például az utca is, és minden terepen lehet okosan és bután viselkedni. Vajon mennyire biztonság tudatosan használjuk ezt a terepet? Ha valakinek ezernél is több barátja van, vajon ismerheti-e személyesen mindet? Hányan lehetnek, aki ötletszerűen telepítenek ismeretlen Facebook alkalmazásokat? Vagy hányan kattintanak olyan linkre, amit egy ismeretlen Facebook partner küldött? Egy új oldalon aztán újra be kell lépni egy Facebook oldalhoz megszólalásig hasonló oldalra, egy óvatlan kattintás után azonban kikerülhet a jelszavunk. A feltört fiókok pedig hasznosak lehetnek a bűnözőknek további, látszólag ismerősök nevében küldött csaló pénzgyűjtő üzenetekhez. Magyarán az ember a postafiókjára, Facebook profiljára nem csak saját maga miatt, hanem ismerősei védelme miatt is kell, hogy vigyázzon.

1.- Ne töltsünk fel olyan képet, ami ciki

Érdemes gondolni arra, ha családi vagy nyaralási képeket töltünk fel, akkor szabályozzuk annak megtekinthetőségét. Itt személyre, vagy csoportokra bontott lehetőségek között lehet választani. Ha ezt nem tesszük meg, olyasfajta kellemetlen élményekre ébredhetünk, mint a választási kampányban némely politikus. Egyre több kamera egyre több felvételt készít egyre több fiatal részegeskedéséről. Az idő múlik, és tisztes családapaként nem hiányzik egy rosszakaró, aki kettétöri karrierünket fiatalkori botlásunk miatt. Vessük az eszünkbe, az adatok a legnagyobb biztonságban akkor vannak, ha egyáltalán fel sem töltjük őket.

2.- Ne posztoljunk ki, ha elmegyünk nyaralni, és üres lesz a lakás

Nagyon sokan a Foursquare segítségével realtime közvetítésként osztják meg életünk minden apró rezdülését a nagyérdeművel, hol járnak, mit csinálnak. A Pleaserobme.com honlap egészen érdekes dolgot mutat meg ezzel kapcsolatban: az általuk mellékelt keresési módszerrel élve magunk is meggyőződhetünk arról, hogy éppen ebben a pillanatban is milyen sokan közlik felelőtlenül pillanatnyi helyzetüket, és a betörők minden bizonnyal örülnek az ilyen részletes online közvetítésnek. Hasonló okok miatt ne posztoljuk ki előre, ha elutazunk, inkább mindig utólag számoljunk be erről.

3.- Időnként fésüljük át a biztonsági beállításainkat

Állítsuk be a Beállítások -> Adatvédelem Beállítások -> Profil menüpont alatt, mit engedélyezünk. A beállításokkal elvileg meghatározhatjuk, kinek és mibe engedélyezünk bejelentkezést. A lehetséges választások a csak a barátok, a barátok és csoportjaim, a barátok barátai, és a mindenki között mozoghat. Sajnos az alapértelmezés gyakran a bátor megosztás, így ha valaki lusta, figyelmetlen, vagy csak mert megijed a rengeteg opció szerkesztésétől, az minden mozdulatát, mondanivalóját kisugározza a Világegyetemnek. Azt is be tudjuk állítani, látszódnak-e a kommentek az összes ismerősünk üzenő falán. Külön beállítható, hogy a kommentjeink, vagy "lájkjaink" a fotóknál, üzeneteknél, linkeknel, videóknál láthatóak legyenek-e mindenki számára, vagy sem.

4.- Szervezzük listára az ismerőseinket

Bárkivel előfordulhat, hogy főnöke, anyósa meghívót küld számára. Ha okosan szervezzük ismerőseinket, akkor külön csoportba tesszük családtagjainkat, munkatársainkat, kollégiumi osztálytársainkat. A listáinkat más nem láthatja, mi pedig könnyen tudunk így egy adott célcsoportnak üzenetet küldeni. Elrontani is nehezebb a címzettet, például elég rosszul veszi ki magát, ha a barátok helyett péntek délutáni "a munkahely nem kocsma, hogy állandóan ott legyünk, indulok is haza" üzenetünk a munkatársaknál, főnököknél landol.

5.- Állítsuk be kereshetőségünket

Lehetőség van beállítani az Adatvédelem -> Keresés menüpontnál, mi látszódjon. Nyilván adatvédelmi szempontból az a legrosszabb, ha fotótól kezdve ismerőseink listáján át azokig az oldalak listájáig, amelynek rajongói vagyunk. Tartozik ez tényleg másra? Sajnos mindenki az "én csak egy hétköznapi átlagember vagyok, nincsenek értékes titkaim" téveszmében él, és ontja a muníciót magáról. Aztán mindenki meglepődik, ha később már politikus jelöltként előéletére ráuszítják a kompromittáló kommandót, vagy leendő munkaadója ellenőrzi korábbi netes megnyilvánulásait esetleg matematikus-statisztikus szakemberek profilt építenek számára testre szabott reklámküldés céljából.

6.- Használjunk hosszú és erős jelszót

Sokféle hibát követhet el egy átlagfelhasználó, és ebből az egyik a primitív jelszavak használata. Az "abc", "123" vagy "admin" típusú jelszavak nem védenek semmi ellen sem. Egy jól kitalált karaktersorozat ingyen van, és ennek fontosságát nem lehet elégszer hangsúlyozni. Korábban már szóba került például a Conficker féreg kapcsán, hiszen ott is a támadás egyik módszere éppen a hálózati gyenge jelszavak elleni szótáralapú támadás.

A Webroot egy korábbi, átfogó felmérés keretében mintegy ezeregyszáz Facebook-, MySpace-, Twitter-, Linkedlin-felhasználót kérdezett ki a webhasználati szokásairól. Körülbelül 36 százalékuk ugyanazt a közösségi portálon alkalmazott jelszavát máshol is használja, egynegyedük (28%) fogad el barátkérőt idegentől, valamint 30% nem rendelkezik vírus és kémprogram elleni védelemmel. A közhiedelemmel ellentétben a feltört accountokat nem varázslatos hackereszközökkel, hanem a harmatgyenge jelszavak szimpla kitalálásával szerzik meg legtöbbször. A jelszóval való törődés nem azért van, hogy bosszantson minket, hanem hogy sikerrel szolgáljon, védjen bennünket, amit meg is tesz, ha mi is gondosan állunk hozzá. Ha rendszeresen cseréljük, kellően erőset választunk és nem ugyanazt használjuk mindenhol, máris sokat tettünk - saját magunkért.

7.- Ne facebookozzunk nyitott wifiről

Az ESET Magyarország felmérése szerint a magyar internet-felhasználók 58 százaléka alkalomadtán barátja vagy munkatársa számítógépét használja e-mailjei ellenőrzésére, 34 százalékuk pedig nyilvános számítógépekről is belép postafiókjába. Emellett a felhasználók 10 százaléka ismerősei számítógépén is bankol, 4 százalékuk pedig különböző - például internetkávézóban elhelyezett - nyilvános számítógépeket használ utalásainak elintézésére. A legbiztonságosabb, ha kizárólag saját számítógépünket használjuk levelezésre, Facebookozásra és banki ügyeink intézésére. A nyilvános számítógépek többségére szinte bárki telepíthet olyan kémprogramot, ami ellophatja jelszavainkat.

8.- Ne installáljunk mindent válogatás nélkül

Volt már korábban egy Fan Check nevű csaló Facebook alkalmazás, amely elméletileg profilunkon keresi meg, hogy mely ismerősünk írt/kommentelt a legtöbbet a dolgainkra. A gyakorlatban ehelyett azonban a kezdőlap összezavarását lehetett tapasztalni. Nem egyedi eset a Fan Check, idővel divat lett a dologból a Facebook kiegészítők háza táján, és ezekből a kártékony kisalkalmazásokból azóta rengeteg létezik már. Néhány éve keletkezett egy vakriadó a Facebookon, amiben arra hívták fel a figyelmet, ha valaki egy "unnamed app", magyarul névtelen alkalmazás nevű holmit talál magánál, akkor azonnal törölje, mert az állítólag kémprogram. Persze nem az, de az már az ötletgazdák képzelőerejét dicséri, hogy a Google találatok kártevőkkel való mérgezésével rákészülték a szituációra, ha az egyszeri Facebook júzer rákeres az "facebook unnamed app" kulcsszóra. A tapasztalat azt mutatja, sajnos nem érdemes arra számítani, hogy majd gondos kezek Facebooknál gyorsan kitakarítják a gyanús, kártékony linkeket, alkalmazásokat, hiszen van, amikor hónapok, vagy akár évek is eltelnek.

9.- Ne kattintsuk le a megdöbbenítő híreket, ne kattintsunk a chatben sem ismeretlen linkekre

Bármit lehet ígérni a Facebookon, ahogy olyan érdekességet is, amelynek a címe például: "Az emberek 98 százaléka nem tudja 17 másodpercnél tovább nézni ezt a videót". Aki annak idején bedőlt ennek, és rákattintott a captcha-nak álcázott képre, az akaratlanul is megosztotta ismerőseivel a kártékony linket. Azonnal a csoport rajongói közé került, és nevében ismerősei üzenetet kaptak, melyben a fenti videót ajánlja figyelmükbe. Tulajdonképpen semmilyen videó nem létezett, helyette viharos sebességgel nőtt a kártékony oldal rajongói tábor. Ha egy "very shocking", vagy "must see it" Facebook

videót csak akkor lehet megnézni, ha előtte lájkolni vagy csatlakozni kell, inkább mondjunk le róla. Ha egy Facebook videót csak akkor lehet megnézni, ha előtte engedélyeznie kell egy ismeretlen alkalmazás telepítését, amely természetesen hozzá akar férni az üzenőfalhoz, ismerőseinkhez, személyes adatainkhoz, inkább mondjunk le róla. És még egy fontos dolog: ha üzenetet kapunk látszólag egy barátunktól, nem biztos, hogy ő küldte. Ha például nem ír semmit, csak egy linket küld, majdnem biztos, hogy az kártevőre mutat. Ha pénzt kér, akkor pedig szintén csalásra lehet gyanakodni, például feltörték vagy megfertőzték ismerősünk gépét, és most végig levelezik az ismerőseit az ő nevében.

10.- Csatlakozzunk a facebook.com/biztonsag oldalhoz, ahol rendszeresen értesítenek az új veszélyekről

A <http://facebook.com/biztonsag> oldalon keresztül az ESET magyarországi képviselete folyamatosan gyűjti a Facebook átveréseket, az oldal rajongóit pedig figyelmezteti ezekre. Ha szeretnénk folyamatosan értesülni az új biztonsági tippekről, vagy értesítést kapni arról, ha megjelenik egy átverés a Facebookon, akkor csatlakozzunk az oldalhoz és a Tetszik gomb megnyomásával tegyük be az oldalt a kedvenceink közé.

Hogy milyen lábnyom marad utánunk, azt jól szemlélteti a következő példa, amiben már a big data és a cégek célzott adatbányászata is szerepel. „A Target áruházlánc weboldalán elhelyeztek egy regisztrációt a várandós nők részére, amivel különféle célzott többlétszolgáltatásokhoz, kuponokhoz jutnak néhány adat megadása után. Ezeket az adatokat elemezve jött rá a cég, hogy a kismamák a második trimeszter kezdete táján nagy mennyiségben vásároltak szagtalan testápolót, illetve az első 20 hétben az átlagnál nagyobb mennyiségű kalcium, magnézium, és cink tablettákat. A szülés közeledtével pedig megnőtt az illatmentes szappan, az extra méretű vattalabda-csomag, és a kézfertőtlenítő vásárlásaik száma. Összesen 25 olyan terméket lokalizáltak, amelyek kombinációit vásárlók esetében a rendszer kiadott egy terhességi valószínűségi mutatót, valamint azt, hogy az adott kismama a terhesség milyen szakaszában tart és mire lesz szüksége a későbbi szakaszokban. Ezt az algoritmust pedig nem csak a webes regisztrálók esetén, hanem a hagyományos vásárlóknál is elkezdtek használni és terhes termékeket tartalmazó kedvezménykuponokkal ajándékozták meg őket. Egy nap bement egy felháborodott férfi az egyik áruházukba, és dühösen követelte, hogy a vezetővel beszélhessen. Felháborodott, hogy a középiskolás lányának terhességi termékeket tartalmazó kuponokat küldött az áruház, ezzel "arra csábítva" a gyereket, hogy idő előtt vállaljon gyereket. A felháborodott apukát sűrű elnézéskéresekkal sikerült leszerelni, a szoftver fejlesztőket pedig gondolom alapos fejmosás érte. De mikor néhány nappal később az ügyfélszolgálat még egyszer visszahívta, az apa már más hangnemben beszélt, mivel időközben kiderült, hogy apuka féltve őrzött, kicsi lánya valóban terhes, de neki nem merte elmondani. Az apuka természetesen megdöbben, hogy az áruház előbb tudta? A szoftver azonban a szokások alapján helyesen mutatta ki a várandósságot.”

És végül, ne csak technikai összefoglaló legyen ez az egész, ezt is érdemes megszívlelni felnőtteknek, gyerekek egyaránt: „Több kommunikáció kevesebb tömegkommunikáció! Meg persze több szeretet.” (Kerekes Bernadatte)

Nem csak akkor szerepelhet rólunk fotó, ha azt mi magunk töltöttük fel, ez is egy nagy tanulság. Ismerőseink, más gyerekek szülei is megteszik ezt általában sajnos a tudtunk és jóváhagyásunk nélkül. De a nyilvános koncerteken, előadásokon, konferenciákon is készülnek felvételek, és gyakran a jegyvásárlás apró betűs részében benne van, hogy a vásárlással ezzel is egyetértünk és hozzájárulunk.

Összefoglaló szabályok:

- ne tiltsuk
- Beszélgessünk a gyermekkel!
- Ismerjük meg virtuális barátait!
- Rendszeresen ellenőrizzük adatlapját!
- Kérjük meg, ne álljon szóba idegennel!
- Kérjük meg, hogy ismerős felvételét és fotó megosztását előbb beszélje meg velünk!
- A mások által, de rólunk készített fotók leszedését is kérhetjük a Facebook-tól.

7. fejezet: Chatelés, üzenetküldés, sexting

Kulcsszavak: chat, chatequette, chat roulett, grooming, sms, mms, Snapchat, Messenger

Tények: Sosem lehet biztosan tudni, kivel chatelünk. És nem mindenki az, akinek látszik. A személyes adatok védelme pedig sohasem tökéletes.

a Snapchat esetében szomorú, hogy mennyien elhitték a 10 másodperces képüzenet megsemmisítési ígéretet. Itt meg lehet említeni például a Snaves Android alkalmazást és a hasonlókat, melyek segítségével a tíz másodperces korlátozást megkerülve gyakorlatilag le lehet menteni bármit. A piactereken elvileg zajlik az ilyen appok kiszűrése, kérdés hogy milyen gyorsasággal és hatékonysággal történik mindez. De 2014-ben meg nem erősített utalások szerint a snaves.com weboldal feltörésével került ki ezúttal 13 GB mennyiségű privát fotó, melyek közül sok állítólag kiskorúakat ábrázol.

Egy 2016-os kutatás eredménye szerint a Snapchat lett a legnépszerűbb közösségimédia-alkalmazás a tinédzserek körében. Az alkalmazás megelőzte a Twittert, a Facebookot, de még az Instagramot is. A kutatásban 6,500 amerikai tinédzsért kérdeztek meg, és a válaszok alapján 28%-uk a Snapchattet, 27%-uk az Instagramot, míg a maradék a Facebookot és a Twittert nevezte meg.

Mi a chat? Élő beszélgetés számítógépen, billentyűzve. Ez nem csak névvel végezhető - mint például a sokak által ismert Skype. Különbő chat-szobákban névtelenül is végezhető, ahol mindenki olyan álnevet használ, amelyet akar, bárki bármit mondhat. Ilyenkor érdemes észben tartani, hogy semmi sem titkos, hiszen mások is láthatják, amit írunk.

A „ne tegyünk mással olyat, amit nem szeretnénk ha velünk tennének” jegyében létezik egy „Chatiquette”, vagy magyaros adaptációja "netikett" néven. Ebben olyan hasznos tanácsokat találunk, mint például: „Viselkedj úgy, mint a valós életben! Add meg a tiszteletet mindenkinek! Először olvass, csak utána írd! Ne sértegetsz és ne rágalmaz másokat! Soha ne írd mérgesen!”

Mik a chat veszélyei? A gyerekek naivak és hiszékenyek! Ismeretlen, rosszindulatú emberek bújhatnak meg a kedves nevek mögött, akik esetleg ismerősnek vagy gyerekkorúnak hazudhatja magát. Beszélgetés közben alaposan kifaggatja a gyermeket (lakcím, szülők anyagi helyzete, stb.) de durván, trágárul beszélhet, sőt akár öngyilkosságra buzdíthat, vagy drogot árulhat. Sajnos tipikus átverés az is, hogy meztelen képet kér a gyerektől, akiket aztán további szexuális szolgáltatásokért vagy pénzért megzsarol. Ha pedig tiltakozik, akkor azzal fenyeget, hogy beárulja a szüleinek vagy nyilvánosan lejáratja. Sajnos sok öngyilkosság történt már hasonló esetek miatt, az egyik leghíresebb Amanda Todd esete.

Semmi bizalmasat ne ossz meg, hol laksz, hova jársz iskolába, otthon vannak-e szüleid, ki vigyáz rád, szüleid bankszámla vagy kártyaszámát. Az is jótanács lehet, hogy lehetőleg moderátoros chat szobákat használjunk, ahol durvaság, vagy probléma esetén

beavatkozhatnak az üzemeltetők. Ne fogadj ismeretlenektől fájlokat, ugyanis gyakoriak a vírusok, kémprogramok.

Lehetőleg soha ne találkozz az interneten megismert emberrel. De ha mégis, úgy előzze meg több másik, alternatív kommunikáció is: pl. Skype, e-mail, stb. Mindig vigyél magaddal készpénzt, mobilt, és egy megbízható (felnőtt) kísérőt! Fontos, hogy valaki más is tudjon róla, hogy miért és hova mentél! Nyilvános helyre menjtek és kerüld a kihívó öltözködést!

A Sexting nem más, szexuális tartalmú szöveges, képes vagy mozgóképes üzenetek. Egyszerűbben fogalmazva önmagukról és vagy partnerükről jellemzően mobiltelefonnal készített (fél)meztelen, erotikus kép. Egy 2014-es felmérés szerint az amerikai felhasználók 50%-nak van a telefonján pucér képe másokról, főképp 14-24 életkorban. Ezek a tartalmak könnyen feltölthetők mobillról az internetre, illetve a telefon ellopása után is kerülhetnek illetéktelen kezekbe, szóval óriási veszélyforrás.

Idézet egy internetes cikk kommentjei közül, sajnos nagyon jellemző manapság: „Ismerősöm fia 14 év alatti létére szexuális zaklatóként kerülhet bíróság elé, mert kéretlenül küldött meztelen képet magáról egy csajnak. És ez nem egyedi eset... Igen, az akarat (a hormonok, stb...) bennünk is megvolt fiatalon hasonló baromságokra, de soha a történelemben nem lehetett meg ezt ilyen egyszerűen megtenni. Elektronikusan minden sokkal könnyebb, hatványozottan igaz ez az okostelefonnal. „

Pedig ezek a törvényi előírások vonatkoznak rá:

SEXTING - Btk. 207. §: 18 éves kor alatt tiltott pornográf felvétel és kész.

- megszerezni, tartani 0-3 év
- készíteni, kínálni, átadni 1-5 év
- kereskedni, nagy nyilvánosság számára hozzáférhetővé tenni 2-8 év

De rajtunk kívül álló okok miatt is kiszivároghat, például a Snapchat 2014. januári feltörése 4.6 millió felhasználót érintett kellemetlenül. A kikerült képeket pedig aztán már bárki láthatja (új "célközönség"): "pedomaci", "tündérmackó" típusú honlapok, ahol ország-világ előtt gyaláznak főleg lányokat.

Szemlátomást egyre fiatalabb korban kezdődik nem csak úgy általában a kütyühasználat - mar óvodások tableteznek -, és az internetezés, hanem a régebben főként inkább az idősebb gyerekekre jellemző nemkívánatos viselkedés is sajnos egyre korábbra kerül. Például a telefonon küldözgetett, csereberélt pucér magukról készített selfiek mar sajnos 11-12 éves gyerekeknél is előfordulnak.

Meg kell mindenkinek tanulni, hogy az internet nem felejt, és ami egyszer felkerült, amit egyszer feltöltöttünk, azt soha többé nem tudjuk letörölni, nem tudjuk megmondani kihez kerülhet még - a címzett is továbbadhatja, elvesztheti - a küldés után gyakorlatilag nincs efelett többé kontrollunk. Sokan egyébként figyelmen kívül hagyják az EULA szövegét, például a Facebook és a Skype esetében a regisztrációval azt is jóváhagyjuk, hogy az

üzeneteink a szolgáltató tulajdonába kerülnek.

Ne használjuk az üzenetküldőket nyitott wifi kapcsolatnál, ekkor ugyanis könnyen lehallgatható a kommunikáció. Emellett a "No platform is safe" jegyében kívánatos az is, hogy minden eszközünkön fusson vírusvédelmi alkalmazás. Ez például az Androidos telefonok esetében is fontos, hiszen sok olyan trójai alkalmazás létezik, amely a háttérben, titokban bizalmas adatokat szivárogtat a távoli támadók szervere felé.

Becslések szerint 700 millióan használják a Whatsapp alkalmazást. A 2016-ban bevezetett titkosítási technológia révén, melyben a kommunikáció, benne a képek, szövegek, videók és telefonos beszélgetések biztonságosak lesznek, még maga a Whatsapp sem látja ezeket. Természetesen egyedi bírói végzés, alapos gyanú esetén a mobilszolgáltatók és a hatóságok a jövőben is hozzáférhetnek ezekhez.

A chatrobotok is felvetnek egy érdekes problémát. A gyerekek körében nagyon népszerűek az ilyenek, például az egyik ilyen a magyarul is tudó Cleverbot. Bárki csetelhet vele - amolyan szimulált mesterséges intelligencia szerűség - és aki egyedül van, vagy csak szórakozni szeretnek, az beszélget vele. A program megjegyzi a látogatók IP címét, és nyilván websüti formájában helyben is eltárol előzményeket, az újabb látogatáskor pedig "emlékszik", kik vagyunk, és korábban miről társalogtunk eddig. A gyerekek a program által adott "suta válaszokat" viccesnek tartják, és folyamatosan igyekeznek egyre mehökkentőbb reakciókat kiváltani a Cleverbotból, amit aztán lementett képernyőképként mint jó poént megosztanak egymással. Mivel sokszor elég extrém vagy intim kérdéseket is feltesznek, a későbbi megosztott információ pedig az "internet nem felejt" miatt később a viccesből akár nagyon kínos is lehet, ami elég aggályos. És valószínűleg azt is csak nagyon kevesen gondolják végig - a gyerekek biztosan nem -, hogy az így elraktározott személyes beszélgetés információknak, előzményeknek - melyek a szolgáltatás szerverén találhatóak - mi lesz a későbbi sora. Mi történik, ha esetleg a webhelyet feltörik, milyen adatvédelmi stratégiát követnek a kezelésükkel, eladják-e ezeket kereskedelmi vagy reklámcégeknek, akik aztán adatbázist építhetnek belőle, stb.

Néhány hasznos szabály a chateléshez:

- Soha ne beszélj teljesen idegenekkel!
- Soha ne ossz meg magadról olyan képet, amelyen hiányos öltözetben vagy, és amiben nem mennél ki az utcára.
- Ne chatelj az éjszakába nyúlóan! Este az ember fáradt, eltompult, és nem rendelkezik teljes ítélőképességével, hajlamos felelőtlenül megosztani olyan információkat, amit máskor nem tenné. Másnap reggel utólag ne kelljen semmit megbánni
- Mielőtt valakivel találkozna, más alternatív kommunikációs csatornán is vedd fel az illetővel a kapcsolatot. Például ha telefon, Skype, e-mail, stb. útján is elérheted, az azt mutatja, hogy az illető valós személy, aki nem rejtőzködni akar.
- Ha valaki olyat kér tőled (pénz, meztelen fotó, bizalmas információ, bűncselekményre akar rávenni, stb.), ami miatt kényelmetlenül érzed magad, haladéktalanul lépj ki a beszélgetésből!

8. fejezet: Webkamera

Kulcsszavak: webkamera, kukkolás, kinect, a dolgok internete, játék konzolok

Tények: 2010-ben egy philadelphiai (USA) iskolában a diákok használatra adott noteszgépeivel kapcsolatosan felmerült a webkamera jogosulatlan használata. Ez úgy derült ki véletlenül, hogy a gépeket üzemeltető iskola több esetben figyelmeztette a diákokat, hogy "otthon helytelenül viselkedtek", és ez ne forduljon elő többet. Kiderült, hogy a tanárok valóban képesek voltak távirányítással aktiválni a tanulók webkameráját, ám erről a lehetőségről a diákok és a szülők szerint egyáltalán nem tájékoztatták őket. Az ilyen behatolásból 14 hónap alatt negyvenkettőt biztosan végrehajtottak a vizsgálatok szerint.

A GoPro sportkamerákat sokan szeretik, és sokan is használják. 2015-ben Ken Munro etikus hacker megmutatta, miként lehet titokban kémkedni, vagy a felhasználó felvételeihez hozzáférni még akkor is, ha a készülék power gombjával azt látszólag kikapcsolták. A kulcs az eszköz "okossága", azaz a wifin keresztüli netes kapcsolathoz található, a gyenge jelszavak itt is csábítják a bűnözőket, hiszen rengetegen használnak ilyen sportkamerákat világszerte. Muro bemutatta, hogyan tudta az asztalra letett, és látszólag kikapcsolt Hero4 kamerát feléleszteni, majd a LED kijelzőt lekapcsolva az eszköz videostream-jét, illetve hangját a mobiltelefonjáról képes volt nézni/hallgatni. Ezenkívül nem csak kémkedni, hanem távolról törölni is lehet a kamerán korábban tárolt videofelvételeket.

A kémprogramok a tudtunkon kívül észrevétlenül is figyelhetnek bennünket. 2013 júniusában számoltak be egy cikkben arról, hogy az alvilági feketepiacon 100 férfi ér egy nőt, és már fillérekekért, 1 dollárért lehet kapni távoli webkamerás hozzáférést lányokat kukkolni.

Védekezésül azt tanácsoljuk, hogy használat után kapcsoljuk ki, húzzuk ki, takarjuk le. Ez érvényes nem csak PC számítógépre, de akár okostelefon előlapi kamerájára, tabletre, Xbox Kinectre, IP kamerára, okostelevízió beépített kamerájára, stb.

Ha külső kamera egységről van szó, húzzuk ki bátran a kábelét, amikor épp nincs használatban. Ha pedig a noteszgép, tablet vagy okostelefon beépített kamerájáról van szó, ragasszuk le a festéshez használt papírragasztóval, melyet később ragasztónyom nélkül könnyen el tudunk távolítani. Az is egy megoldás lehet, ha vásárolunk vagy készítünk rá fedelet, sapkát, és ezekkel takarjuk le, amikor nincs használatban.

Ha nem csak az okos telefont, hanem a tableteket és PC-eket is nézzük, megint csak tény, hogy a kamerával kémkedhetnek utánunk. Villanhat a LED, vagy akár sötét is maradhat, nyilván ez a fajta kíváncsiság most nem a hirdetőktől, hanem a bűnözőktől ered. A feketepiacon egy női felhasználó webkamerájához tartozó hozzáférés árért - ami mindössze csak egy, azaz 1 amerikai dollár - száz férfi használatot kukkoló webkamera hozzáférést lehet kapni. 2013. júniusában például Rachel Hyndman 20 éves glasgow-i lány volt az egyik ilyen áldozat, akinek kedvenc szokása volt, hogy miközben a kádban fürdött,

vitte magával a laptopját, és DVD-t nézett rajta. Egy ilyen fürdőzés közbeni filmezés közben egyszer csak azt észlelte, váratlanul bekapcsolt a webkamera. "Szörnyű érzés volt a privát szféra ilyen fokú megsértése" - mondta el később.

Mit tehetünk mi felhasználók az éppen használaton kívüli kamera kihúzásán, illetve letakarásán felül? A sebezhetőségeket kihasználó kémprogramok miatt feltétlenül fontos rendszerünk javítófoltokkal való frissen tartása, valamint a naprakész vírusirtó, és tűzfal. Ne kattintsunk ismeretlenektől jövő kéretlen üzenetek mellékleteire, ez a leggyakoribb forrása a trójai kártevőknek, kémprogramoknak. Emellett érdemes alaposan meggondolni, mielőtt ismeretlenekkel chatelés közben megosztanánk saját webkameránk képét. Sose vigyünk webkamerás gépet intim helyekre: fürdőszoba, WC, öltöző, a fiataloknak, gyerekeknek pedig tanítsuk meg, mire vigyázzanak, mik lehetnek a kockázatok. Ha pedig esetleg azt tapasztaljuk, hogy támadás áldozatává váltunk, haladéktalanul jelentsük azt a hatóságoknak. Talán ideje lenne mindenkinek felismerésre jutni, hogy használaton kívül "csak a letakart webkamera a jó webkamera".

Méltatlanul kimaradt az előbb az otthoni kamerás eszközeink közül például a Kinectes Xbox, amely ugye mikrofonnal és kamerával ott figyel a nappaliban, és eközben állandóan online van. Állítólag persze csak azt figyeli, mikor akarjuk őt bekapcsolni, de az Amazon webáruház a paranoidabbaknak máris árul hozzá esztétikus takaró redőnykét, potom 9.99 dollárért, amely puha bélésével karcmentesen fed, igaz a hangvezérlés eközben aktív marad, ha nem áramtalanítjuk teljesen.

9. fejezet: Vírusok, férgek, kártevők

Kulcsszavak: vírus, kémprogram, botnet, fertőzés, zombi

Tények: 2015. júniusi adat szerint az egyedi vírus kód minták száma elérte a 317 milliót. Már 2008-ban több bevétel származott az USA-ban a számítógépes bűnözésből és elektronikus csalásokból, mint a kábítószer-kereskelemből: 105 milliárd dollár. A mostani váltságdíjszedő zsaroló programok elődje, a hamis antivírus "biznisz" már korábban is elképesztő jövedelmet biztosított a bűnözőknek, például 2008-ban derült ki, hogy a Bakasoftware bűnszervezet "munkatársai" 32 millió forintnyi összeget kerestek akkoriban fejenként és hetente. Hogy mennyire egyértelmű az alvilág és a számítógépes vírusok, csalások között, arra az is jó példa, hogy 2015. szeptemberében Molotov-koktét dobta a Dr. Web nevű antivírus-cég szentpétervári irodájára, miután az leleplezte és nyilvánosan publikálta egy ATM-es csalás részleteit.

- Kártevők, kémprogramok, botnetek, átverések, csalók is részei az internet világának. Hogyan fertőzhetik meg a gépünket? Erre a kérdésre igen sokféle módzat létezik:
- Adathordozók (USB kulcs, CD, DVD)
- E-mail
- Weboldalak, nem csak warez vagy felnőtt, hanem bármilyen
- Letöltés
- MSN, Skype, Viber, WhatsApp, SnapChat, stb.
- Alkalmazások, Appok, Facebook letöltések

1986-2015

A kártevők fejlődnek, a felhasználói hozzáállás helyben jár, sajnos lassan változik. A számítógépes vírusok történelmében a jelképes nulla kilométerkövet a PC MS-DOS (MicroSoft Disk Operating System) rendszerű gépeket támadó pakisztáni eredetű Brain képviseli, megjelenését az 1986. január 19. dátumhoz kötik. A vírusok megjelenése, és napjaink tömeges terjedése miatt a felhasználóknak is megváltozott az élete, így a biztonságos munkavégzéshez, játékhoz, vagy internetezéshez már alaphelyzetben is hozzátartozik a korszerű vírusvédelem. De ugyanígy új kihívás elé kerültek a számítógép-programozók is, hiszen míg korábban elég volt a kódolásnál a jó végeredményre és a gyors működésre koncentrálni, addig ma már a biztonságos programozás is nélkülözhetetlen eleme lett a szakmának.

A kártevőket már régen nem amatőrök készítik, hanem ez már a szervezett bűnözés legjövedelmezőbb ágazata. Már 2008-ban több bevétel származott az USA-ban a számítógépes bűnözésből és elektronikus csalásokból, mint a kábítószer-kereskelemből: 105 milliárd dollár. Jelenleg pedig az FBI jelentése szerint havonta körülbelül egymillió dollárt kaszálhatnak a titkosító-váltságdíjat szedő kártevőkkel a bűnelkövetők - adómentesen. A vírusirtó cégek víruslaboratóriumaiba napi 100-150 ezer új kártevő minta érkezik, és ennek feldolgozása komoly elhivatottságot és erőfeszítést kíván a szakmától.

Zsaroló programok

A fájljainkat titkosító és azok visszaalakításáért váltságdíjat szedő kártevőből sajnos egyre több keletkezik. Cryptolocker, Cryptowall, CTB-Locker - hogy csak az ismertebbeket említsük. Amennyiben egy ilyen zsaroló kártevő megfertőzte valakinek a gépét, akkor már egyedül csak offline mentésből lehetséges a helyreállítás, ugyanis jelenlegi ismereteink szerint a fájlok dekódolása sajnos a legtöbb esetben nem végezhető el. Ha már egyszer bejutott a gépünkre a kártevő, akkor minden Windows alatt felcsatlakoztatott, betűjellel megosztásként hozzárendelt - külső meghajtónkon is végigfut a titkosításával, így sajnos az összes bedugott USB tárolónk, hálózati meghajtóink, de még a felhős tárhelyünk is áldozatul eshet. Ez pedig még akkor is így van, ha az adott megosztás nem is Windows alapú gépen található, de onnan elérhető.

A célja az egésznek a váltságdíj, amelyet Bitcoinban követelnek a bűnözők. A szakemberek felhívják a figyelmet a Windows rendszerek azonnali frissítésére, és arra, hogy soha ne nyissunk meg ismeretlen mellékletet. Emellett ugyancsak a vírusvédelmi megoldások használata nagy mértékben segíthet, hogy a rendszerünket megvédjük, de ehhez a vírusvédelmi szoftverből mindig az aktuálisan legfrissebb változatát célszerű használni, és természetesen naprakész felismerési adatállományokkal, emellett pedig az antivírusnak a megfelelő beállításokkal - például felhős vizsgálat lehetősége, proaktív ellenőrzés engedélyezése, stb- - kell rendelkeznie. A mentés nagyon fontos, sőt a kulcsa a sikernek: legyen párhuzamosan több különböző verziónk is a teljes (nem inkrementális) mentésekből, tartsuk ezeket offline, akár több különböző fizikai helyszínen is tárolhatjuk őket. És ne kizárólag egyetlen kópia álljon rendelkezésre, amely rendszeresen felülírja az előző egyetlen mentésünket. Ha ugyanis mégis bejutna a fertőzés, akkor így hamarabb találunk korábbi sértetlen állapotot, és nagyobb eséllyel lesz miből válogatni.

Érdekes módon, ha valakinek vírusfertőzött a gépe - például mert elhanyagolja a frissítéseket, egyáltalán nem izgatja magát ezen. Ha a számítógépe egy botnet része, és a távoli támadók ellopják a netkapcsolatának jelentős részét, spammelnek, DDoS támadásokat hajtanak végre az ő zombi gépéről, a felhasználók jelentős hányadát ez sem érdekli. Ám ha a saját adatok - fájlok, dokumentumok, fényképek - titkosításra kerülnek egy zsaroló kártevő miatt, mindenkit azonnal érdekelni kezd a fertőzés.

Elmondhatjuk, hogy ezek a zsaroló kártevők egyre erősebb kulcsokat használva titkosítva felülírják az állományainkat, majd a feloldó kódért pénzt követelve jelentik napjaink legnagyobb veszélyét. Nem is kis összeget, általában 300 eurónak (körülbelül 90 ezer forint) megfelelő summát kérnek, és a 48/72 órás határidő leteltével megduplázódik a váltságdíj összege. Nem árt tudni, ha bejutott a gépünkre egy ilyen titkosító kártevő, akkor ha elegendő ideje van, minden Windows alatt mappelt - értsd felcsatlakoztatott, például betűjellel hozzárendelt - meghajtónkon is végiggyalogolhat a titkosításával, így sajnos az összes bedugott USB tárolónk, hálózati meghajtóink, de még a felhős tárhely is áldozatul eshet. Az esetleges váltságdíj kifizetést a biztonsági cégek - az emberrablási esetekhez hasonlóan - nem javasolják, mert ezzel részint tovább bátorítjuk a bűnözőket. Másrészt erről azt is tudni kell még, hogy mivel nem úriemberekkel vagy Grál lovagokkal üzletelünk, hanem bűnözőkkel, emiatt aztán semmilyen garancia nincs arra, hogy egyáltalán kapunk

valamilyen kódot, vagy az működőképes lesz. A beszámolók jelentős részénél - kb. 80-90%-ban - a fizetés ellenére nem is érkezik semmilyen feloldó kulcs.

10. fejezet: Lánclevelek, álhírek, spamek, csalások, átverések

Kulcsszavak: *hoax, ingyen nyeremény, átverés, emelt díjas SMS, továbbküldés, spam szűrés*

Tények: *A levelek 85%-a spam, azaz kéretlen szemétleve.*

A legfontosabb spam szabály, hogy soha ne válaszoljunk, mert azzal csak megerősítjük a küldők felé, hogy működő címünk van, és akkor sokkal több spamet fogunk kapni, sőt a címünket mint garantáltan működőt továbbadják, eladják. A kéretlen leveleket ne küldjük tovább ismerőseinknek se, akármilyen érdekes, vagy figyelemfelkeltő tartalom szerepel benne.

Fontos tisztában lenni azzal, hogy a kéretlen levelekben sok esetben csalók jelentkeznek, vagy kínálják silány minőségű termékeiket. Az olcsó hamis gyógyszerek, hamisított termékek kifejezetten rossz minőségűek, vagy akár életveszélyesek is lehetnek. „Ingyen” nyeremény sajnos nincs, mindig figyeljük az apró betűt! Sok esetben személyes adatainkkal fizetünk a ki tudja ki által „szervezett” nyereményjátékért, vagy ami már a bűncselekmény határát súrolja, a jóhiszemű részvételi SMS válasz beküldésével valójában egy borsos árú emelt díjas szolgáltatásra iratkozunk fel, amelyet nehéz vagy éppen lehetetlen lemondani.

Mindig gondolkozzunk, és ha valami túl szép, ahhoz hogy igaz legyen, akkor valószínűleg nem is igaz. "Ingyen" afrikai örökség sincs, és Bill Gates sem osztja szét a vagyonát, ép ésszel nem tenne ilyet senki! Nyilvánvalóan valamilyen átverés keretében személyes adatainkat akarják begyűjteni.

Használjunk spamszűrést - például olyan komplett internetbiztonsági csomaggal, amely ezt a modult is tartalmazza. Ha valamilyen weboldalon meg kell adnunk az e-mail címünket - például kapcsolat felvételhez, akkor a kiírt címnél PONT és KUKAC szöveg legyen, ez segíthet a spam-adatbázisba címgyűjtést végző automata robotok ellen.

A Halon amerikai internetezők körében 2013 augusztusában végzett vizsgálatának adatai szerint döntő többségük, egészen pontosan 94.7 százalékuk kapott már olyan e-mailt, amelyben vírus, kémprogram vagy valamilyen kártevő volt. Nagyjából 8.8%-uk meg is nyitotta az ilyen mellékletet megfertőzve ezzel a számítógépet, 30.2% azonban az utolsó pillanatban gyanút fogott. A hamis üzenetek leggyakrabban valamilyen bank nevében érkeznek (15.9%), de előkelő helyen szerepelnek a hamis leveleknél a közösségi oldalak is, például a Facebook vagy a Twitter (15.2%) vagy a különféle online fizetési szolgáltatások 12.8%-ban.

Minden harmadik amerikai beismerte, hogy simán megnyitja az ilyen leveket, ha az üzenet tárgya számára érdekesnek hangzik. A nők inkább a közösségi oldalak nevében érkezőkre harapnak, míg a férfiak jobbra a pénzkereséssel, illetve szexuális témák

esetén esnek kísértésbe. Gyors haszon a tőzsdén, különleges gyógyszer akció, azonnali adó-visszatérítés, Windows crack, kiemelkedő jövedelem napi egy óra otthoni munkával, univerzális szériaszám generátor minden víruskeresőhöz, vagy Kournikova meztelen fotói. Pontosan ezért a 33%-os rátaért jó csalétek a vírusterjesztésben a különféle hírességek meztelen fotóit ígérni. Erre az eredményre egyébként jól rímel az korábbi ESET felmérés, amiből kiderült, a 18-29 évesek 17%-a szokta kikapcsolni a vírusirtóját azért, hogy fertőzött fájlokat tudjon elindítani, 12%-uk pedig azért, hogy fertőzött weboldalakot látogathasson.

Jól tetten érhető, hogy a szűrés ellenére beeső spamek, kéretlen üzenetek már régen nem reklámról, kéretlen értékesítési csatornákról szólnak, ahol hasonmás Rolex órát vagy olcsó Viagrát akarnak ránk sózni. Az ilyen üzenetek fő csapásiránya inkább a megtévesztés, sebezhetőséget tartalmazó melléklet vagy link felkínálása, adatlopás, vírusfertőzés. A levél tárgysorának gyanús kinézete alapján 70%-uk nem kattint rá ilyesmire, azzal is tisztában van 42%, hogy a csupa nagy betűvel írt szöveg szinte mindig kéretlen reklám, ezért elkerülik.

Bár igaz, hogy az ismeretlen feladó, a furcsa nyelvezet, helyesírási hibák, idegennyelvű levél (56%), illetve gyanús formázás is árulkodó jel lehet, azt azért le kell szögezni, hogy tökéletes helyesírású, látszólag ismerősünktől érkező üzenetben is simán kaphatunk kártevőt. Mindenkinek meg kell tanulnia, hogy legyen óvatos, amikor találkozik gyanús e-mailekkel, amelyek eltéríthetik, megfertőzhetik a gépét, illetve pénzt csalhatnak ki tőle, és/vagy ellophatják a személyes adatait is. Erre talán nem is kell jobb példa, mint a 2012-es New York Times szerkesztőség elleni sikeres PDF levél mellékletes incidens, ahol az újságírók megfertőzték a számítógépeiket, és ezzel három hónapon keresztül a kínai támadók minden tevékenységüket távolról láthatták, ellenőrizhették.

11. fejezet: Cyberbully - online bántalmazás, zaklatás

Kulcsszavak: állandó online, online bántalmazás, online zaklatás, iskola, mediáció, digitális lábnyom, privát szféra

Tények: Egy 2014-es felmérésből az derült ki, hogy a brit szülők 54 százalékának fogalma sincs arról, ha a gyereket az interneten keresztül zaklatták. Ez azt is jelenti, hogy a legtöbb szülőnek nincsenek a kezében megfelelő eszközök, hogy időben felismerje és kezelje ezt a gyerekekre egyre gyakrabban leselkedő problémát. Az ESET kutatásából az is látható, hogy tavaly csaknem 45 ezer gyerek hívta fel a ChildLine nevű segélyvonalat, a szakértők szerint azonban ennél jóval többen, a gyerekek többsége találkozik az online zaklatás jelenségével az élete során. Ennek ellenére a szülők 52%-nak ötlete sincs, hogy mit tegyen, ha kiderül, hogy a gyereke áldozattá vált.

A kutatók szerint szinte már csak a pszichopaták kommentelnek. 2016. márciusában Austinban volt egy SXSW tech fesztivál, ahol szó esett az internetes zaklatásról is. A Pew Research kutatásai szerint az internethasználók 40 százalékát érte már online zaklatás, ennek elszenvedői főleg a 18-28 év közötti fiatalok, náluk a zaklatások aránya eléri a 65 százalékot. Az emberek 12.9 százaléka nyilatkozott úgy, hogy fenyegették már fizikai erőszakkal is online. A CiviliNation nevű szervezet kutatása szerint ezek a támadások főleg a Facebookon érik őket. (The Guardian/444.hu)

Gyurkó Szilvia, gyermekjogi szakértő szerint a gyerekek felnőtt segítség hiányában nagyon sokáig titkolhatják, magukban tarthatják a problémáikat. Ezért nagyon fontos beszélni arról a gyerekeknek, hogy vannak jó titkok és rosszak. Az a titok, ami belülről rág vagy feszít, az rossz. Azt nem szabad magunkban tartani. Ha viszont a gyerekek nem találnak olyan személyt - akár egy megbízható barátot -, akivel meg merik osztani a korábban rejtegetett, titkolt élményüket, akkor akkorára hatalmasodhat a probléma, és annyira kitöltheti az áldozat életét a szorongás, hogy a kétségbeesés miatt tragikus lépésre szánhatja el magát. Ilyenkor jut eszükbe "megoldásként" a szökés, a kábítószer, vagy az öngyilkosság.

Az Oktatási Jogok Biztosának 2009-es Iskolai veszélyek című jelentéséből az derült ki, hogy az iskolákban sok a verés, a kiközösítés, és a megszegényítés. Az akkori adatok szerint minden középiskolás osztályban volt legalább 2-3 olyan diák, akiket valamilyen formában kiközösítettek, és osztályonként egy gyereket kis raboltak az osztálytársak. Minden ötödik középiskolás rúgta vagy ütötte meg valamilyen osztálytársát, és egy részük egyedül vagy csoportosan elkövetett veréssel rendezte le vitás ügyét. Harmaduk számolt be arról, hogy a közösségben valamilyen nyilvános megszegényítés áldozata lett.

Becslések szerint a gyermekbántalmazásról készült fotók száma az interneten több tíz millióra tehető. A szülők a technológia terén erőteljesen lemaradtak gyerekeiktől, emiatt nem tudnak megfelelő segítséget nyújtani nekik. Mindezt az arctalan bűnözők erőteljesen kihasználják, de a gyerekeknek saját kortársaik is sok sérülést okoznak. Zaklatásnak sokféle megjelenési formája lehet, például a személyes- és intim adatok/fotók megszerzése és az ezekkel való visszaélés, de a lejáratás, megfélemlítés, a kérértlen és bántó levelek küldözgetése is, vagy a megaláztatásokról készült fotók, videók nyilvános

megosztása is gyakori.

A kutatások szerint a magyar tizenévesek negyedét érte már online zaklatás, és európai átlagban a magyar gyerekek teszik közzé magukról a legtöbb információt: 53%-uknak teljesen publikus a profilja.

Magyarországon az online erőszak nem kap kellő figyelmet: míg a szülők tudni akarják, ha az iskolában, játszótéren, offline közösségben csúfolják, kiközösítik, bántják a gyerekeket, addig az online életükkel egyáltalán nem foglalkoznak. A szakemberek szerint ennek fő oka, hogy a szülők és a gyerekek egészen másként használják az internetet. A szülők nincsenek tisztában a veszélyekkel, nem ismerik és nem ismerik fel az online erőszakot, és gyakran maguk is rossz példát mutatnak személyes adataik nyakló nélküli felelőtlen megosztogatásaival.

Az online zaklatás sokkal gyakoribb mind a külföldi, mind pedig a magyar iskolákban, mint a hagyományos iskolai fizikai bántalmazás. A statisztikák szerint mindegy ötödik gyerek áldozatul esik ilyen cselekménynek. Leggyakrabban a személyes adatok illegális, beleegyezés nélküli közzététele, valamint a különféle online oldalakon - például közösségi felületeken - való megszegyenyítés, fenyegetés, kiközösítés fordul elő.

Sport az állandó zaklatás, beszólás, nincs hova elbújni. 24/7 online jelenlét.

Cyberbully - online bántalmazás, zaklatás

- az úgynevezett cyberbully nem csak külföldön, de itthon is mindennapos
- vitathatatlanul minden területen megváltoztatta az életünket a számítógép
- és ez a gyermekekre is hatással van
- sok rossz inger érheti őket
- ezenkívül a társas, közösségi, társadalmi kapcsolatok is mások, mint régen
- régebben valakit csúfoltak, tudott róla az osztály, vagy többen az iskolából
- most ha megosztanak egy megalázást, az egész iskola, az egész település tudhatja, láthatja, növeli a frusztrációt.
- ami egyszer az internetre felkerül, sosem lehet leszed
- ne felejtsük el, éretlen, kibontakozóban lévő, önmagukat kereső fejlődésben lévő személyiségekre micsoda rombolással lehetnek osztály, város vagy egész internet előtti szidalmazása, csúfolása, megszegyenyítése
- nagy a látencia, az esetek többsége észrevétlen, bejelentetlen marad
- a prevenció a leghatékonyabb módszer
- a legfőbb hadszíntér az iskola
- akik fizikailag is agresszívak, azon az online térben is ugyanezt teszik
- a szerepek nem különülnek el élesen, aki az egyik felállásban áldozat, az egy másikban támadó is lehet
- ha zaklatás történik, nem elhallgatni kell, az a legrosszabb
- bátorítani kell a bejelentést, ez NEM árulkodás. A jogos szóvá-tétel nem panaszkodás.
- bár a szülők többsége nem tud technikai kérdésekben segíteni, de gyerek-szülő viszonylatban tud

- létezik kék vonal chat, email és telefonvonal formájában, safer internet program, ahol felkészült családsegítők, pszichológusok anonim módon állnak rendelkezésre, adnak tanácsokat 24 órában

Az online zaklatás (cyber bullying) mindennapos jelenség az interneten: az elkövetők számítógép vagy okostelefon segítségével igyekeznek megfenyegetni vagy kellemetlen helyzetbe hozni áldozataikat.

Az ESET kutatásából kiderült, hogy 2015-ben csaknem 45 ezer gyerek hívta fel a ChildLine nevű segélyvonalat, a szakértők szerint azonban ennél jóval többen, a gyerekek többsége találkozik az online zaklatás jelenségével az élete során. Ennek ellenére a szülők 52%-nak ötlete sincs, hogy mit tegyen, ha kiderül, hogy a gyereke áldozattá vált.

A kutatási eredmények kapcsán a hazai helyzet sem sokkal biztatóbb. Az online zaklatás nálunk is egyre komolyabb fenyegetést jelent a gyerekek számára, annak ellenére, hogy a szülők többségének ismeretlen ez a jelenség, mivel a legtöbbjüknek sosem kellett ilyesmivel szembenéznie korábban.

Az online zaklatás és a zaklatás egyéb formái közti fő különbség, hogy előbbi esetben a zaklató a biztonságot nyújtó gyerekszobában is elérheti áldozatát. Ez pedig akár jóval ijesztőbbé is teheti ezt a jelenséget, hiszen a gyerek nem tud elmenekülni előle. Szerencsére hazánkban is egyre többen ismerik fel ennek a témának a veszélyét, így egyre szélesebb réteget érnek el a biztonságosabb internetezésre oktató információs kiadványok.

A kutatás készítői arra is kíváncsiak voltak, hogy a szülők hogyan kezelnék a helyzetet, kihez fordulnának, ha a gyerekeik online zaklatás áldozataivá válnának. A válaszok megoszlása a következő volt: a válaszadók 45%-a a gyerek iskolájában keresné a megoldást, 70% kapcsolatba lépne a zaklatás helyszínéül szolgáló weboldallal, míg 38%-uk emellett magával a zaklatóval is felvenné a kapcsolatot.

Az online zaklatás kezelésére a legjobb módszer beszélgetni a gyerekekkel és megismerni az adott helyzet részleteit. A szülőknek meg kell értetni a gyerekeikkel, hogy az ilyen típusú fenyegetésekre nem szabad reagálni, azonban, az efféle üzeneteket nem szabad törölni, hogy a későbbiekben bizonyítani lehessen, hogy online zaklatás történt. Számos módszer van, hogy az online zaklatókkal szemben fellépjünk, azonban ezek függenek a zaklató személyétől is.

Ha a zaklatást egy, az iskolába járó másik gyerek követi el, a tanárokhöz kell fordulni. Ha egy ismeretlen, akkor az internetszolgáltató ügyfélszolgálatán kell jelezni a problémát, mert ilyen esetben meg tudják oldani, hogy az illető ne tudjon kapcsolatba lépni a gyerekekkel. Szerencsére nálunk csak ritkán adódik olyan súlyos eset, amikor a rendőrséghez kell fordulni, ám külföldön több ezzel kapcsolatos öngyilkosság is történt már. Magyarországon a KékVonal chat, illetve telefonszámon tudnak a gyerekek anonim módon tanácsot, illetve segítséget kérni, ha zaklatás éri őket.

Az ESET szakértői nyolc arany szabályt fogalmaztak meg a szülők és a gyerekek online biztonsága érdekében:

1. Elengedhetetlen a rendszeresen frissített antivírus és internet-biztonsági szoftver használata.
2. Ugyanilyen fontos a számítógép vagy okostelefon, illetve táblagép operációs rendszerének (OS), illetve alkalmazásainak rendszeres frissítése.
3. Szülőként legyen résen és figyelje, hogy gyermeke milyen tartalmakat látogat az interneten. Védje jelszóval a számítógépet, az internet használatát pedig csak akkor engedélyezze, amikor időről időre rápillanthat a monitorukra. Fontos, hogy az internet-használatnak pontos szabályai legyenek, amelyeket a gyerekek betartanak.
4. A gyereket fontos megtanítani a személyes adatok védelmének (privacy) fontosságára: a szülők ne engedjék, hogy a gyerekek megadják személyes adataikat ismeretlenek, különböző weboldalakon, közösségi hálózatokon vagy üzenetküldő szoftveken keresztül.
5. A ma már számos számítógépbe, laptopba épített webkamera is biztonsági rés lehet. Húzza ki, vagy fedje le a kamerát, amikor nem használja. Léteznek olyan rosszindulatú programok, amelyek a felhasználó tudta nélkül hozzáférnek a webkamerához, illetve, ha hasonló szoftver korábban már megfertőzte a gépet, azt akár távolról is el lehet indítani. A gyerekek csak megbízható ismerősökkel – a szülők által is ismert barátaikkal vagy családtagokkal – való kommunikációra használják a kamerát.
6. Ha a gyerekek a közösségi oldalak használata során az általuk megosztott tartalmakat mindenki vagy a barátok ismerősei számára is elérhetővé teszik, a szülőnek már nincs kontrollja afelett, hogy ki és milyen adatokhoz fér hozzá a gyerekkel kapcsolatban.
7. Az internetre kikerülő információ örök, az internet nem felejt. Ne gondolja senki, hogy ha egy fotót, vagy akár egy közösségi háló teljes felhasználói fiókját kitörli, akkor a kapcsolódó adatok eltűntek a világhálóról. Lehet, hogy a fotókat, bejegyzéseket, vagy hozzászólásokat valaki már korábban lementette a saját gépére. A gyerekek és a szülők is gondolják meg többször is, hogy milyen fotókat vagy adatokat tesznek elérhetővé magukról az interneten.
8. A szülőknél meg kell érteniük, hogy a gyerekek számára az internet nem egy eszköz, hanem élettér. Ezért rendszeresen beszéljék meg gyerekeikkel, mi történt ott velük, ahogy azt is megkérdezzék, mi volt a játszótéren, vagy a fociedzésen. Az is hasznos, ha a szülők is valamennyire képzik magukat a számítógépes biztonság területén, hogy gyermekeik számára hasznos tanácsokkal tudjanak szolgálni.

Iskolai zaklatás - tanárok is a célkeresztben

Sokszor és sokat beszéltünk már gyermekeink védelméről, a biztonságos

internethasználat oktatásáról az iskolákban. Az ilyen előadások, képzések, rendkívüli osztályfőnöki órák csak részben szólnak szigorúan vett számítástechnikai ismeretekről, a másik mondanivaló az bennük, hogy a mai modern eszközök világában - pl. a szinte mindenkinél jelenlévő okostelefonos diktafon, fényképező, filmfelvevő birtokában, vagy a pillanatok alatt milliókhoz eljutó hírek és képek a közösségi hálózatok világában - hogyan lehet etikusan, emberségesen, biztonságosan megóvni a naiv és veszélyeztetett kiskorúakat megalázástól, pedofiloktól, zaklatóktól, kiközösítéstől, erőszakos tartalmaktól.

Azonban zaklatás, lejáratás áldozatává nem csak a gyerekek, hanem maguk a tanárok is könnyen válhatnak. Megváltozott világunkban az oktatás is gyökeresen más körülmények között zajlik, a már emlegetett technikai fejlődés következtében gyökeresen átalakult. A már óvodás koruk óta a szülők tabletjét, okostelefonját, játékkonzolt és számítógépet használó gyerekek szinte mindegyikének van már saját okostelefonja. Ebben a környezetben a tanárok helyzete is teljesen megváltozott a még szigorú tekintélyvel tükröző 90-es évekhez képest. A diákok ma már nem csendben ülnek, hanem előadás közben folyamatosan neteznek, csetelnek, messengereznek, facebookoznak, sőt igazából valós időben ellenőrzik a tanár mondandóját a Google-val és azonnal beszélnek, ha szerintük esetleg téved valamiben.

Rendszeresen fordulnak elő az iskolákban olyan incidensek, amelynek tanárok az áldozatai. Például 2015-ben egy brit, West Sussexi illetőségű középiskolai tanár, Philip Stack, aki egy Photoshops durva támadás áldozata lett. Az elkövetők a középiskola Twitter fiókjának feltörése után belemontírozták az iskola igazgató fejét egy alsónadrágos férfit ábrázoló fényképbe, és az alábbi üzenetet posztolták a nevében: "Round of applause for our magnificent head! Been working hard in the gym and got himself a contract with Brazzers!". Vagyis "Tapsoljuk meg a mi csodálatos főnökünket. Kemény edzőtermi gyúrás után szerződést ajánlottak neki a Brazzers-nél." (A Brazzers egy pornográf weboldalt üzemeltető montreali cég). Az incidens egy vasárnapi napon történt, és azt csak később vették észre, amikor is aztán leállították az iskolai Twitter oldalt. Az igazgató az eset után a rendőrséghez fordult, hogy találják meg az elkövetőket.

Nem új keletű ez a probléma, hiszen 2011-ben például egy nevadai iskolában, Carson Cityben az egyik 12 éves tanuló szervezett a tanáraik ellen ilyen elektronikus támadást, aminek még nevet is adott: "Attack A Teacher Day". Barátaihoz és osztálytársaihoz intézett felhívást - mintegy száz tanulóhoz - hogy csatlakozzanak és együtt hajtsák végre azt. Tizennyolcan ezt jó bulinak tartották - egyikük még azt is írta, hogy halál rájuk - és válaszukban támogatásukról biztosították a középiskolás lányt. Hatukat azonban a tervezett nap előtt felkeresték a hatóságok és letartóztatták őket. A lányok akkor azzal védekeztek, hogy mindez csak ártatlan tréfa volt, és a rendőrség sürgősen túl komolyan vette azt.

Egy angliai iskolai szervezet, az ATL felmérése szerint pedig már 2009-ben is a tanárok mintegy 15 százaléka szenvedett el valamilyen számítógépes zaklatást tanulóiktól vagy azok szüleitől, negyedüket pedig vádolták már meg hamisan.

Az nyilvánvaló, hogy az interneten bárkinek a fotóival vissza lehet élni, hamis profilt, vagy az illetőt rossz színben feltüntető álhíreket lehet létrehozni - ebből a tanárok irányába a hamis pedofil-vád a legdurvább -, vagy üzenetekben fenyegetni is könnyű őket, és ezeket pusztán csak technikailag megakadályozni sajnos gyakorlatilag lehetetlen.

Azt mindenki döntse el maga, hogy ezek a változások mennyiben jók, mennyiben újak, mások mint régen: a Facebookos lejáratások csupán átvették a székre tett rajzszög helyét, vagy egy egészen új irányt vett a tanár-diák viszony, amit valamilyen szinten muszáj kordában, egészséges határok és törvényes keretek között tartani.

Aáry-Tamás Lajos, az oktatási jogok biztosa az Országgyűlés kulturális bizottsága előtti 2015-ös meghallgatásán közölte, évente 1500-1600 panasz érkezik hivatalához. Már az óvodákból is egyre több panasz érkezik, de a gyerekek az internetes kiközösítéstől is félnek. A gólyatábori ügyekből az látszott, hogy az agresszió az egyetemeken is jelen van. Az ombudsman elmondta: 522 panasz érkezett szülőktől, 705 tanulóktól, 162 pedagógusoktól, intézményvezetőktől, oktatóktól. Emellett egy 2015-ös felmérés szerint a zaklatást a kamaszok 43% a kábítószerrel való visszaélésnél is súlyosabbnak tartja. 18%-uk már volt zaklatás áldozata, 38%-uk viszont nem mondta el a szüleinek, és az áldozatok ötöde gondolt az öngyilkosságra.

Szabályok zaklatás esetére:

- Ha valaki chat-en, e-mailben zaklat, ne töröld és ne válaszolj, tedd el a levelet bizonyítéknak!
- Te se zaklass másokat, és ha mást zaklatnak, ne továbbítsd!
- Jelentsd a problémát az üzemeltetőknek, tiltsd le, blokkold a küldőt!
- Szólj róla a barátaidnak, szüleidnek, tanáraidnak!
- Segíts a barátodnak, ha ő kerülne ilyen helyzetbe!
- Szükség esetén fordulj a hatósághoz!
- Vigyázz a jelszavadra, ügyelj a biztonsági beállításaidra!

A pedagógusoknak pedig azt kell megérteniük, hogy élethosszig való tanulás rájuk is vonatkozik, ha értik az internetes világot, akkor tudják hatékonyan megóvni a rájuk bízott gyerekeket. Nem mellesleg pedig felelősségük is van ezzel kapcsolatosan:

„Kiskorú veszélyeztetésének büntetése a Btk. értelmében

A 2012. évi C. törvény a Büntető Törvénykönyvről (Btk.) 208. §

„(1) A kiskorú nevelésére, köteles személy – ideértve a szülői felügyeletet gyakorló szülő, illetve gyám élettársát, ha a kiskorúval közös háztartásban vagy egy lakásban él –, aki e feladatából eredő kötelességét súlyosan megszegi, és ezzel a kiskorú testi, értelmi, erkölcsi vagy érzelmi fejlődését veszélyezteti, bűntett miatt egy évtől öt évig terjedő szabadságvesztéssel büntetendő.”*

** Természetesen ide kell érteni a gyermeke nevelésével, oktatásával megbízott pedagógust, a szakoktatót és a tanulók felügyeletével megbízott más iskolai alkalmazottat is.”*

Végezetül ismét csak számokat mutatunk, mennyire széleskörű és fontos ez a jelenség. Következzen egy idézet brit "Ditch the Label" zaklatásellenes szervezet statisztikájából, amely a fiatalokat érintő online megfélemlítéssel és zaklatással kapcsolatban végez rendszeres felméréseket, ezek a 2014-es adatok.

- 10-ből 7 fiatalnak online módon
- 37% nagyon gyakran esik áldozatul online zaklatásnak
- 20%-a naponta kénytelen meg tapasztalni valamilyen durva online zaklatást
- az eredményekből világosan látszik, hogy a fiúk és lányok egyaránt veszélyeztetettek
- a fiatalok véleménye szerint a Facebookon kétszer annyira erős a jelenség, mint más közösségi hálón.
- a megkérdezettek 54%-a élt már át a Facebookon online megfélemlítést vagy zaklatást
- a Facebook, a Twitter és az Ask.FM a legnagyobb, és egyben a legerősebb terepei a zaklatásnak
- az internetes zaklatásnak komoly későbbi hatásai vannak/lehetnek a fiatalok önbecsülésére, ezt tapasztalta a felmérés válaszadóinak 70%-a
- egyes becslések szerint az Egyesült Királyságban naponta 5.4 millió online zaklatás történik, és 1.2 millió gyermek ezt rendszeresen, naponta kénytelen elszenvedni

12. fejezet: Szexuális bűnözők

Kulcsszavak: pedofília, Interpol, szexuális ragadozók, grooming, chat, ismerősnek jelölés

Tények: A nyelvi elemzés területén is működnek már törvényszéki szakértők, akik többek közt például a névtelen fenyegetők elleni nyomozásokban adnak tanácsot a hatóságoknak, illetve a szöveghasználat jellegzetességeiből - például chatszobák beszélgetési szövegeiből - tudják igen nagy hatékonysággal kiszűrni a rejtőzködő pedofilokat.

Adatok a prostitúcióról: Az állami gondozott gyerekek 70 százaléka érintett a prostitúcióban, és a felnőtt prostituáltak 40 százaléka gyerekként kezdte. Hazánkban kb. 15 ezer prostituált dolgozik, többségük szeretne kiszállni, de nem tud. A gyermekkorú prostituáltak 80 százalékát 10 éves kora előtt szexuálisan zaklatták.

2015-ben 5835 kiskorú menekült tűnt el Németországban. Luise Amstberg, a Zöldek frakciójának menekültügyi szóvivője ezzel kapcsolatban azt mondta, aggasztó, hogy a kormány nem veszi komolyan a prostitúcióra kényszerítés és a kizsákmányolás egyéb formáinak veszélyét, amely az eltűnt kiskorúakat fenyegeti.

Az ingyenes internetes pornó korában a mai fiatalok nagy eséllyel előbb találkoznak ezekkel az anyagokkal, minthogy saját szexuális tapasztalatokat szereznének.

A 2014-es magyarországi bűnügyi statisztika 4,163 "gyermekek érdekeit sértő vagy család elleni bűncselekményt" tart nyilván. Magyarországon 2014-ben a rendőrség 16,885 fiatal- és gyermekkorú eltűnése ügyében adott ki körözést. A rendőrségi adatok szerint a gyerekek körülbelül fele pár órán belül, még az eltűnés napján vagy másnap meglesz, a többiek jelentős része pedig nagyjából egy hónapon belül. Viszont az eltűntek közül minden évben nagyjából százan sajnos soha többé nem kerülnek elő, az ő sorsukat örökre titok övezi. ORFK Hermon nevű körözési rendszere alapján készült nyilvántartás adatai szerinti a 2015-ös esztendőben 16,429 14-18 éves és 2,850 14 év alatti fiatal eltűnésével kapcsolatban indult nyomozás, ez együtt 19,279 eltűnt gyereket jelent.

Egy nemzetközi szervezet (2016. ECPAT International Global Study, Ministry of Foreign Affairs of the Netherlands) tanulmányából az derült ki, hogy az utóbbi 20 évben egyre több gyermek szenvedett el szexuális bántalmazást. A tanulmány szerint a gyermekek szexuális kizsákmányolása a világ minden térségében probléma, és a korábbi jól behatárolható viszonyokat (például jól szituált, gazdag, nyugati országokból érkező idősebb fehér férfiak tömeges utazása ázsiai országokba) felváltották a teljesen kiszámíthatatlan viszonyok. Nincs tipikus elkövető, jellemző helyszín, vagy térség. Az életünkben bekövetkezett rengeteg változás - szabad utazási lehetőség, turizmus, civilszervezetek önkénteseinek tömeges részvétele gyerekekkel kapcsolatos projekteken, politikai menekültek áradata, alkalmi és vendégmunkások állandó jelenléte éppúgy átalakította életünket, mint az internet széleskörű használata, valamint titkosított és anonimizálást szolgáló technikák elterjedése.

Először is szögezzük le, hogy az internetes pedofília - Bűncselekmény! Mire használják ők az internetet? Ismerkedésre, konspirált kapcsolattartásra, tiltott pornográf anyagok

terjesztésére. Tudatosan előre felépített taktika jellemzi őket: előbb bizalmat ébreszt, majd személyes találkozóra hív. Az ilyen atrocitások pedig egy egész életre szóló traumát okoznak, például Pamela Anderson 35 év után hozta nyilvánosságra, hogy fiatal korában zaklatták.

Mit tehetünk mi felnőttek? Elsősorban beszéljünk a gyermekkel, ismerjük meg virtuális barátait, rendszeresen ellenőrizzük adatlapját. Kérjük meg, ne álljon szóba idegennel, és ha képet akarna megosztani, vagy új ismerőst szeretne felvenni, azt előtte beszélje meg velünk. Szerencsére az üldözésben vannak nemzetközi együttműködések, hatásos eredmények is a magyar és külföldi hatóságok, többek közt az Interpollal is jó a kapcsolat.

- Sajnos az országoként különböző jogszabályok nehezítik, pl. gyerek modell oldalak. Más országban az ilyen tilos, viszont Magyarországon legális, emiatt magyar tárhelyeken tartják az ilyen fényképeket a nemzetközi bűnözők.

2016 januárjában egy szexuális bűnöző letartóztatásában segített egy éber anya, aki 15 éves lánya Facebook partnerei közül szúrta ki az ismeretlen, leveleket írogató idősebb férfit. Gyanús lett számára, hogy ez az ismeretlen partner már a legelső levelében is meztelen képeket kért, és a személyes találkozási lehetőségről érdeklődött. Egy üzenetben az anya megkérdezte tőle, helló, mennyi idős vagy, és a válasz az volt: 33 éves. Kis netes nyomozással aztán hamar kiderítette, hogy a 33 éves férfi nem túl okosan az igazi nevét használta, ám az igazi meglepetés csak ekkor következett.

Dennis Williamset ugyanis hat évvel korábban már elítélték, mert kiskorúakról terjesztett szeméremsértő anyagokat, magyarul pedofil tartalmakért. Az aggódó anyuka ezek után haladéktalanul értesítette a helyi rendőrséget. A rendőrséggel együttműködve immár a nyomozókkal karöltve mégis megszervezték a "személyes találkozót", ahol aztán letartóztatták a bűncselekménnyel vádolt férfit. A helyi rendőrség szerint Williams addigra már tömegesen kereshette a fiatakorú lányok ismeretségét az interneten, ezért külön felhívást és figyelmeztetést tettek közzé a szülőknek, hogy mindenki legyen óvatos, és ellenőrizték gyermekeik partnereit közösségi oldalon. A grooming, vagyis a bűnelkövetők által a szóba jöhető áldozatok feltérképezése, behálózása és becserkészése sajnos nagyon is gyakori jelenség.

Idézzünk egy, a kiskorú lányokat segítő Névtelen Utak Alapítvány munkájával foglalkozó cikkből: „A kamaszlány elszökik az intézetből, várja őt a nagyvilág és a pultos munka Hollandiában – de már a tizenévesek is pontosan tudják, az ilyen utak nem a diszkóba, hanem a bordélyba vezetnek. A gyermekkorukban megerőszkolt, később a gyermekotthonból elcsábított, kurvának eladott lányok története a világ egyik legnagyobb tabutémája. Tízből tíz lány veszélyeztetett, hetet el is adnak prostinak. Az okok megértéséhez nem csak olyasmiket érdemes vizsgálni, mint a mélyszegénység, a gyerekkorban történt szexuális zaklatás és az, hogy az érintetteket jellemzően még soha nem szerette senki, soha nem voltak olyan közegben, ahol fontosnak érezhették magukat, így a későbbi stricik, a „loverboyok” könnyen el tudják csábítani őket pusztán azzal, hogy

törődnek a lányokkal. ”

Egy amerikai vlogger, Coby Persin egy elég egyszerű kísérletben mutatta be, hogy egyáltalán nincs nehéz dolguk a pedofiloknak. A szülők engedélyével egy 12, egy 13 és egy 14 éves lánnyal kezdett el beszélgetni Facebookon. 15 éves fiúnak adta ki magát, és minden gond nélkül kapta meg a címet, az egyik lány pedig még az autójába is beszállt, annak ellenére, hogy sohasem látta a fiút. Először csinált egy kamuprofil, aztán bejelölt három lányt. A 13 éves Mikayla minden félelem és távolságtartás nélkül beszélgetett az idegen fiúval. Pár nap után Persin találkozót kért, amire a lány igent mondott. Még azt is elárulta, hogy a szülei nincsenek otthon, és a házukhoz legközelebbi parkban beszélte meg a randit. Ahogy a lány odaért, az apja rögtön leordította, milyen veszélyes dolgot művelt. A második esetben nagyjából ugyanez történt. A 12 éves Julianna könnyen beleegyezett, hogy találkozzon az idegennel. Csak egy dolgot kötött ki, akkor kell találkozunk, amikor apukám nincs otthon. Felhívta magához Persint, aki apukával nyitott ajtót. Elmagyarázták neki, hogy nem a legszerencsésebb beengedni bárkit a lakásba. A Facebookos fiú egy szexuális bűnöző is lehetett volna. A legelszomorítóbb a harmadik lánynál történt. A 14 éves Jenna szintén hamar találkozott Persinnel, aki a háznál vette fel. Jenna gondolkodás nélkül igent mondott a kocsis randira, simán beszállt a furgonba, pedig nem is látta az ülésen azt a fiút, akivel az interneten beszélt. Hátul a szülei várták, akik sokkot kaptak, mennyire egyszerű volt elcsalni a lányukat. Amerikában több mint 750 ezer regisztrált pedofil él, akiknek még a kisujjukat sem kellett volna megmozdítaniuk, hogy találkozzanak ezzel a három lánnyal. Az említett videót - The Dangers Of Social Media (Child Predator Social Experiment) Girl Edition! címmel - ezidáig már több, mint 45 millió látták a YouTube oldalán.

A felvételen látható utólagos szülői kiabálás valószínűleg a félelem miatt tört elő, sajnos csak arra jó, hogy a gyerek az apjától féljen, és emiatt meg inkább mindent titkoljon, mással beszéljen meg mindent. Ha minden nap nyugodt körülmények között megbeszelnék, mi történt az "online térben", akkor lehet, hogy sosem fajulna idáig a dolog. Pedagógiai szempontból pont ez lenne a lényeg, hogy ne azért ne csináljon ilyet, mert fel az apjától, vagy a büntetéstől, hanem mert sikerül vele megértetni, és felismeri milyen veszélyt rejthet magában egy ilyen helyzet. A Biztonságos Internethasználat Gyerekeknek (B.I.G.) oktatás azért jó, mert felmutatja a "döntések - következmények" vonalat. Aztán utána úgyis azt csinálnak, amit akarnak. Az igaz, hogy egy kicsit valóban TV show szerű a dolog, meg Amerika, de: ha a valós életben "csak" egy gyerek is így lépre menne, már az is szörnyű. És gyanítható, hogy tv show mentesen és ország függetlenül sajnos bőségesen meglenne egy legalább 10%-os arány. Szülőknek érdemes lenne megnéznie, mert kicsit sem baj ha még idejében ezen meg idejében mindenki eltöpreng kicsit.

A szexualitás terén sok minden változott, de felvilágosítás miatt érzett prűdéria, szégyen, vagy egyéb okok miatt ez a terület ma is sok helyen „kényesnek”, elkerültnek számít. Nem szabad azonban a szülőknek annyira naivnak lenni, hogy azt gondolják, ha feléjük nincs kérdés, akkor máshol nem próbálnak kérdezni. És a szexualitás területén a pornográfia is erőteljesen belépett. Egyfelől bárki számára könnyen elérhető, másfelől az aki nézi,

tévesen azt gondolhatja, ebből kellene elsajátítani a nemi szerepeket, a viselkedést, a szokásokat, a szereplők tényleg így viselkednek a való életben: kiszállítják egy idegen címre a pizzát, aztán 2 perc múlva már orgiát rendeznek. Sok durvaságot is innen tanulnak, ezért az iskolai szexuális felvilágosítás órán ezzel a témakörrel is érdemes (lenne) foglalkozni, és elmondani, hogy azok, akik szeretik egymást és szeretkeznek, az egészen más, mint amit a pornó filmek alapján sokan gondolnak.

Egyes országokban igen szigorú szabályokat alkalmaznak a pedofilekkel szemben, például akár halálbüntetésre is ítélik, kémiai (tablettákkal való) kasztrálásra, és elektronikus nyomkövetők viselésére kötelezhetik őket. A kémiai kasztráció állítólag megszünteti, illetve drasztikusan csökkenti a szexuális vágyat. Ilyen például Csehország, Lengyelország, Dél-Korea, Ausztrália és Indonézia, de ezeket a módszereket alkalmazzák számos amerikai államban is.

13. fejezet: Bankolás, online vásárlás

Kulcsszavak: bank, két faktoros azonosítás, virtuális bankkártya, fizetesközvetítők, utalás

Tények: A bankkártyás visszaélések száma rendkívül nagy gondot jelent Magyarországon is: az MNB legfrissebb adatai szerint csak 2014-ben tízmilliárdos károkat okoztak a bankkártyás bűnözők.

Egy korábbi felmérés tanúsága szerint mi magunk is óvatlanok vagyunk, a felhasználók 10 százaléka ismerősei számítógépén is bankol, 4 százalékuk pedig különböző - például internetkávézóban elhelyezett - nyitott wifis nyilvános számítógépeket használ utalásainak elintézésére. A nyilvános számítógépek többségére szinte bárki telepíthet olyan kémprogramot, ami ellophatja jelszavainkat. Ezért ezeken lehetőleg ne adjuk meg jelszavainkat, és semmiképpen se lépünk be internetbankunkba.

A netes vásárlás egyszerű, 0-24, időt, pénzt, energiát takaríthatunk meg. Létezhet néhány hátrány: csekély információ a termékről, ismeretlen eladó, bizonytalan tranzakció - de ezek inkább az ismeretlen weboldalak, webshopok jellemzői. A nagy látogatottságú, biztonságos fizetéssel rendelkező, széles körben ismert, leinformálható áruházak - Amazon, Alibaba, stb. - teljes biztonságot nyújtanak, garanciával. Bármit is vegyünk, fontos hogy nézzünk utána az eladó/kereskedőnek, tájékozódjunk a teljes költségről (pl. szállítás, vám miatt lehetséges felár), keressük meg, mik az adott oldalon a nyújtott garanciális feltételek, illetve a fizetési módok, és azok biztonsága is lényeges információ.

Fizetés:

- Figyeljünk arra, hogy https alatt, vagyis a kis lakattal jelzett titkosított kapcsolattal lépünk be. Sok helyen érhető már ez el, sőt alapértelmezetten adott nem csak a https titkosított kapcsolat, hanem a kéttényezős hitelesítés is: a Google, PayPal, Yahoo, Twitter, Facebook, az Apple ID, és a Snapchat is rendelkezik ezzel, érdemes tehát használni.

- Itt jöhet jól például a két faktoros azonosítás, amely a banki ügyletek esetében is elterjedt, és használata megnehezíti a bűnözők számára az életet. Ennek lényege, hogy ilyenkor a szokásos név-jelszó páros beütése után igénybe kell venni egy jelszógeneráló eszközt is (tokent vagy mobiltelefonra érkező SMS aláírást), ami egy egyedi, egyszer használatos jelszót generál. Vagyis ilyenkor a támadónak még a telefonunkat is el kellene lopnia, hogy ehhez hozzáférjen. (Persze mattot így is sokféleképp adhatunk magunknak: nyitott wifivel, nyilvános helyen a vállunk felett kifigyelhető adatainkkal, hanyagul kezelt elvesző telefonunkkal, stb.)

- Virtuális kártyás fizetés, PayPal fizetesközvetítő

Elvileg a fizetesközvetítő cégek éberren figyelnek arra, ha valaki elégedetlen a vásárolt áruval, vagy szándékosan becsapják. Ekkor ugyanis a szerződő partnerek kötelesek biztosítani a pénz-visszafizetési garanciát, ellenkező esetben gyanússá válhatnak, illetve a fizetesközvetítő (pl. PayPal, AlertPay, stb.) ideiglenesen vagy véglegesen kitiltja őket, és akkor ezzel elzárja előlük a pénzcspot. De szintén elvileg azt is figyelik, ha valahol pedig

túl nagy számban történik reklamációs pénzvisszafizetés, akkor ott valószínűleg kétes üzelmek zajlanak. Ezért aztán a csalók igyekeznek minél tovább pedánsan a „nem feltűnő, megfelelő” szinten tartani ezeket a mutatóikat. Sőt, ezen felül több számlát használva, vagy ezek rendszeres, például havi csereberejével is operálnak a nehezebb lelepleződés érdekében.

Ha valaki nagyon mérgesen, az üzletmenetet veszélyeztetve fellép a saját érdekében, a számla folyamatossága és a botrány elkerülése érdekében a hőzöngőket gyorsan kártalanítják jól tudva, a nyereség maximalizálása érdekében megéri ez a kis áldozat az esetek 1-3 százalékában, mert a fizető csendes többség szégyenében, idő hiány miatt vagy mert esélytelennek érzi nem panaszkodik, nem fordul hatóságokhoz, hanem lenyeli az egyszeri veszteséget.

12 tipp a biztonságos online vásárláshoz

Az online vásárlás folyamatosan, évről évre nagyobb teret nyer az, egyre többen veszik igénybe, a webáruházak forgalma pedig meredeken emelkedik. Természetesen ezzel a csalások száma is növekszik, kiberbűnözők lesik áldozataikat, hogy a szeretet ünnepének nevében kellemetlen pillanatokat szerezzenek több ezer figyelmetlen vásárlónak.

Összeállításunkban csokorba gyűjtöttük azokat a kihagyhatatlan és nélkülözhetetlen biztonsági tippeket, amelyekkel biztonságosabbá tehetjük az online vásárlást, és elkerülhetjük, hogy az internetes rendelés, webáruházás vásárlás csalódással, esetleg átveréssel végződjön. A biztonsági tanácsok természetesen nem csak a kiemelt ünnepi időszakokban érvényesek, bátran alkalmazzuk őket egész évben.

1. Készítsük fel a számítógépünket és digitális eszközeinket!

Szeressük a számítógépünket! Legyünk hozzá is jók, és mielőtt nekiveselkednénk a karácsonyi nagybevásárlásnak, tegyük rendbe az eszközt. Lássuk el frissített, komplex védelemmel, frissítsük és javítsuk a böngészőnket és a beépülő alkalmazásokat (plug-inek, java, flash stb.) és természetesen az operációs rendszert is.

2. Óvakodjunk az ismeretlen oldalaktól!

Amennyire tudunk, tájékozódjunk előre. Csak megbízható, leinformálható, konkrét címmel, telephellyel, adatvédelmi nyilatkozattal rendelkező portálokon, webshopokban rendeljünk, vásároljunk. A megbízható háttérű, saját vagy ismerőseink által korábbi kedvező visszajelzésekkel rendelkező, pontos szállítási határidőt kínáló ismertebb helyeken mindig nagyobb az esélye a zökkenőmentes bevásárlásnak, de akár a minőségi reklamációnak is, mint egy névtelen, arctalan, postafiók jellegű oldalnak, kínálnak akár elképesztően kedvező áron portékákat.

3. Védjük jelszóval (de ne ugyanazzal) eszközeinket!

Egy év eleji felmérés szerint ötből négy felhasználót zártak ki különböző oldalakról jelszával kapcsolatos probléma miatt. Bármennyire is csábítóan egyszerű az újabb regisztrációhoz ugyanazt a korábbi jelszót megadni, mint amit levelezőnkben, a Facebook-on, vagy bárhol máshol már használunk, sose tegyük! Tippünk: a karácsonyi online vásárlásokhoz rendszeresítsünk egy új e-mail címet, így az ünnepek utáni promóciós e-

mailek hadától is megkíméljük magunk!

4. Győződjünk meg a biztonságról!

Amikor egy oldalon már a rendelési folyamatnál járunk, mindig ellenőrizzük, hogy a szabványos biztonsági tranzakciós csatornát, vagyis az SSL-t használjuk-e. Ezt jelezheti például, ha a böngésző címsorában a http alapprotokoll helyett a titkosított https protokoll jelenik meg, vagy ha a böngésző ablakában egy lakat vagy egy kulcs szimbólum látható.

5. Inkább PC-ről, mint telefonról vásároljunk!

Az előbb említett biztonságos SSL kapcsolat sokkal könnyebben ellenőrizhető egy asztali számítógépen, mint egy tableten vagy egy okostelefon apró kijelzőjén, így helyezzük magunkat kényelembe otthon a gépünk előtt és rendeljünk inkább onnan! A PC-n ezenkívül jobban láthatóak a linkek és az is, ha valahova észrevétlenül megpróbálnak átirányítani minket.

6. A „kihagyhatatlan ajánlatokat” kezeljük fenntartással!

Ha egy ajánlat túl szép ahhoz, hogy igaz legyen, akkor valószínűleg nem is az, főleg, ha ez a szezon egyik legnépszerűbb termékére vonatkozik. Még akkor is, ha nagyon csábítóak ezek az ajánlatok, ne vásároljunk olyan helyen, ahol hihetetlenül olcsón árulnak termékeket, szolgáltatásokat. Az ingyen dolgok ajánlgatása pedig (amely amúgy az egyik leggyakoribb spam), és az emellé társuló sürgetés (pl. csak gyorsan, mert elfogy, csak az első x ember kaphat) tipikus jellemzője az átveréseknek, hogy ne maradjon időnk az ellenőrzésre, a józan végiggondolásra. Ezért ha gyanús linket kapunk, ne kattintsunk rá közvetlenül, hanem írjuk be a böngésző keresősávjába a honlap címét, és így győződjünk meg az oldal valódiságáról.

7. Ne vásároljunk hotspotokon keresztül!

Lehetőség szerint nyilvános, ingyenes wifiről ne rendeljünk árukat, ne gépeljük be személyes és banki adatainkat.

8. Gyerekbarátok a legújabb kütyük?

Ma már természetes, hogy a kisgyermek is digitális kütyüket kapnak ajándéka. Mielőtt gyermekeinknek óriási örömet okozva odaadjuk az ajándékot, győződjünk meg arról, hogy a megvásárolt digitális eszközben található-e beépített gyermekvédelmi program, amelynek segítségével szűrhetjük a gyermekeink által elérhető online tartalmakat. Sok kütyü tartalmaz ilyen beállítási lehetőségeket, mégis nagyon kevés szülő él ezekkel. Legyünk figyelmesebbek!

9. Használjunk elektronikus kártyát a vásárlásokhoz!

Minden banknál létezik külön internetes vásárlásokhoz való elektronikus (unembossed card) kártya, amelynek a számát bátran megadhatjuk akár még a három jegyű ellenőrző kóddal együtt is, ám erre az alszámlára csak a vásárlás előtt közvetlenül netbankunkon vezetjük át a vásárláshoz szükséges pontos összeget, ami csak pár percig lesz rajta, egyébként a számla üres. Ezzel nem tudnak tőlünk lopni, és megadni sosem az igazi

bankkártyánk adatait kell.

10. Vigyázzunk a sok személyes információt kérő oldalakkal

Ha egy webáruház regisztrációjánál úgy érezzük, hogy túlságosan sok, és a vásárlás szempontjából nem releváns adatot is kérnek tőlünk, akkor azonnal fogjunk gyanút, és hagyjuk el az oldalt. Érdekes ilyenkor egy teljes vírus és kémprogram ellenőrzést is lefuttatni a gépünkön.

11. Ingyen kapott pénz még az interneten sem létezik

Ha vásárlás közben egy weboldal vagy még inkább, egy felugró pop-up ablak adatok, űrlapok kitöltögetése fejében értékes ajándékot, iPhone-t, iPad-et, "ingyen pénzt" vagy egyébeket ajánl, távozzunk.

12. Az ünnepek után is maradjunk figyelmesek

Karácsony és Újév közti szünetben a hitelkártya egyenlegeket legtöbbször nem szívesen olvasgatják, talán mert nem szeretnének szembesülni azzal, hogy mennyit költöttek. Pedig az online vásárlás közbeni csalások, átverések során keletkezett kár a számlaegyenlegen mutatkozik meg először. Ha igénybe vesszük az azonnali SMS értesítési lehetőséget, percre készen láthatjuk a terheléseket és a pillanatnyi egyenlegünket a számlánkon. Minél előbb vesszük észre a gyanús tranzakciókat, és teszünk bejelentést, annál nagyobb az esély a szabálytalan ügyletek felderítésére, és ezzel együtt pénzünk esetleges visszaszerzésére.

2009-ben Steve Jobs Amazon áruház accountja akadt horogra, pontosabban ennek kihorgászása az elkövető Orin0co nevű hacker szerint már 2008-ban megtörtént, csak a nyilvánosságra hozatal lett későbbi esemény. A támadó létrehozott egy hamis Amazon áruház weblapot belépéssel, és kifürkészte az ide érkező adatokat. A sok hétköznapi jogosultsági adat mellett azonban nagy meglepetésére maga Steve Jobs is figyelmetlen volt, és besétált a csapdába: megadta a nevét, címét, bankkártya adatait, telefonszámát, valamint Amazonas belépési nevét és jelszavát. A hiteles belépésről képernyőmentés is készült, és a támadó levelet is írt a "bestseller" Jobsnak, amiben azt is megemlíttette, 6-7 évre visszamenőleg még plusz érdekes információ lehet Jobs korábbi vásárlásainak listája. A levélben részletesen elmondta, hogyan sikerült a fenti módon bejutnia és felajánlotta, hogy egyfajta váltságdíjként vegye meg tőle ezeket az adatokat.

A pénzutalások is lehetnek veszélyesek, például ha azt valaki terrorszervezetek javára teszi. 2016. márciusában kezdődött Sydney-ben egy olyan 16 éves lánynak a pere, aki a vádak szerint 10 ezer ausztrál dollárt utalt át Szíriába az Iszlám Államnak a Western Unionon keresztül. A lány - aki 20 éves szíriai származású barátja kérésének tett felelőtlenül eleget - terrorizmus finanszírozása miatt akár 25 év börtönbüntetést is kaphat.

Érdekes a gyerekekkel megállapodni valamilyen rendben. Sokuk már nagyobb korban rendelkezik saját bankkártyával, de fiatalokként elvileg nem vásárolhatnak internetes webáruházban a felhasználói szerződés értelmében. Mondjuk egy érték határ felett kérje

ki a jóváhagyásunkat, beszélje meg velünk. És még egy érdekes adalék. Egy 2015-ös brit felmérés eredménye azt mutatta, hogy a szülők negyede (25%-a) már virtuális valutában, Bitcoinban adja a gyermekének a zsebpénzt. Azt viszont ezzel a helyzettel tudomásul kell venni, mivel a Bitcoinban végzett tranzakciók a hatóságok által is nehezebben követhetőek a hagyományos pénzmozgásoknál, gyermekünk pénzköltése is kikerül így a szülők látóteréből. Adott esetben a zsebpénzéért például drogokat, fegyvert, vírusokat, gyógyszereket, szexuális szolgáltatásokat, szerencsejátékot - szinte bármit vásárolhat nyomtalanul a darknet-nek nevezett alvilági piactereken.

És végül, de nem utolsósorban érdemes szót ejteni a bankkártya jelszaváról is, a PINK kódról. Itt nem csak az a fontos, hogy ne a kártyára legyen írva, vagy mellette egy cetlire, hogy az esetleges tolvajnak megkönnyítsük a dolgát, hanem az erős PIN kód is fontos. Egy régebbi felmérés szerint ugyanis sok ember itt is lusta, és a password, admin és egyéb könnyen kitalálható valódi jelszavakhoz hasonlóan itt is túlságosan egyszerűen megjegyezhető, ezáltal túlságosan egyszerűen kitalálható választ. Az emberek közel 11%-ának 1234 a PIN kódja, de az 1111, vagy a 0000 is sokszor szerepel, így biztosak lehetünk abban, hogy a csalók ezeket biztosan kipróbálják majd. Legjobb, ha nem szerepel benne ismétlődés, nem jegyezzük fel a kártyánkra, letakarjuk a kezünket a begépelésekor, nem áruljuk el senkinek, és ha több kártyánk is van, akkor mindegyikhez egyedi kódot választunk.

Ha spamként, azaz kéretlen szemétlevelelben kapunk ajánlatokat, gyanakodjunk. Jellemzően az ilyen kampányoknak a célja az adathalászat, „GLS csomagod érkezett”, „ingyen iPad”, olcsó iPhone vásárlás, és hasonló levelek ömlenek naponta mindenki postafiókjába. Mindenesetre a vásárlásainkat lehetőleg ne ilyen kéretlen levélajánlatok alapján intézzük.

14. fejezet: Informatikai higiénia

Kulcsszavak: vírusirtó, „no platform is safe”, integrált biztonsági program, tűzfal, védekezés, végpont védelem

Tények: Az FBI jelentése szerint havonta körülbelül egymillió dollárt keresnek a Cryptolocker, Cryptowall és hasonló személyes adatokat titkosító, és a feloldókulcsért váltságdíjat szedő bűnelkövetők - adómentesen. A Bitcoinban követelt pénzdíjak összege is emelkedőben van, eleinte még jellemzően 700 amerikai dollárt kértek, ez nagyjából 200 ezer forint. Ám később a CTB-Locker például Bitcoint kért, ami nagyjából 1680 USD, vagy is már 460 ezer HUF.

A Snowden incidens után sokan elgondolkodtak a számítógépes biztonságon. Egy 2015-ös amerikai felmérés szerint az ottani lakosság változtatásokat, és lépéseket tettek a kémprogramok elleni nagyobb védelmük érdekében. Eszerint 25% használ azóta bonyolultabb jelszavakat, 17% megváltoztatta adatvédelmi beállításait a közösségi médiában, 15% félelmében már ritkábban használja a közösségi oldalakat, illetve 15% az incidens óta szándékosan elkerül bizonyos megbízhatatlannak vélt alkalmazásokat és szolgáltatásokat.

- Vírusirtó

Manapság sokkal inkább használatos az úgynevezett komplex internet biztonsági csomag, mint az ennek csak egy kis szeletét tartalmazó szimpla vírusirtó. Ezek a védelmi megoldások a vírusvédelem mellett spamszűrést, kétirányú tűzfalat, böngészés közbeni védelmet, karantént, adathalászat elleni modult, banki védelmet is nyújtanak, így sokkal hatékonyabban képesek megvédeni a számítógépet. 100%-os védelem azonban nem létezik.

- A tűzfal (angolul firewall) feladata, hogy a számítástechnikai eszközbe ne történhessen illetéktelen behatolás a hálózaton keresztül. Míg a Windows XP tűzfala annak idején csak a befelé irányuló forgalmat szűrte, ma már kétirányú, öntanuló szabályrendszerrel, illetve policy szabályokkal irányítható tűzfalat szoktunk használni, ami naplózni is tud. A riasztások, alapján illetve a napló tételekből lehetőségünk van a gyanús forgalmak azonosítására és kiszűrésére. Az úgynevezett Internet Security komplett biztonsági csomagokban rendre szerepel már a tűzfal modul is, ezek azért is előnyösebbek a különálló programoknál, mert az integrált komponensek tudnak kommunikálni, például a víruskereső motor "tud beszélgetni" a tűzfal komponenssel.

- Legális szoftverek

A védekezés egy másik pillére a legális szoftverek területe. A média állományokkal - film, zene - szemben a fizetős szoftvert nem lehet ingyen letölteni saját használatra. Ez magyarul azt jelenti, hogy az adott céljainknak megfelelő szoftvert megvásároljuk, vagy pedig kereshetünk valamilyen kompromisszum keretében egy kisebb tudású, de ingyenes alternatívát. Sokak számára például bőségesen elegendő egy Microsoft Office irodai csomag helyett egy ingyenes LibreOffice, vagy a szintén fizetős Photoshop helyett a

Paint.NET. A vírusvédelem története jól példázza, hogy a legrosszabb kombináció az, ha a fenti lehetőségek helyett valamilyen lopott, warez szoftvereket használunk. Ugyanis a bűnözők előszeretettel csomagolnak bele a hamis szoftverbe kártevőket, vírusokat, kémprogramokat.

Azt minden esetre fontos tudni, hogy a jelenlegi megállapodások értelmében, melyet a kormány és a Microsoft kötött, minden diáknak ingyenesen és jogszerűen jár a mindenkori legújabb Office változat, amelyet a tanulók Windows, Android, vagy iOS platformra is letölthetnek a www.o365.educatio.hu weboldaltól.

- Frissítések, sebezhetőségek - A számítógépes biztonságnak elengedhetetlen része az operációs rendszer, és az alkalmazói szoftverek hibajavítási foltjainak haladéktalan letöltése és telepítése, hiszen a kártevők előszeretettel használják ki ezeket a javítatlan biztonsági réseket. Ehhez nem csak az operációs rendszer, hanem a különféle alkalmazások (Adobe Flash-től Java-n át Wordpressig) hibajavításait is mindig időben futtassuk le. A frissítetlen rendszerek ellen tömeges és automatizált kampányok keretében zajlanak támadások, melynek során nagy számban fertőznek meg távolról számítógépeket, vagyis nem kell Obama elnöknek lennünk ahhoz, hogy a mi is áldozatok legyünk.

- Mentések: nagyon fontos

Az a legfontosabb, hogy a legnagyobb hangsúlyt a megelőzésre tegyük, mert például egy fizikai meghibásodásnál, vagy zsaroló kártevős támadásnál a mentés sokszor nehézkes, vagy időnként akár nem is lehetséges. Ebben leghatékonyabban a rendszeres és alapos mentés segíthet minket.

Miért fontos a rendszeres és külső adathordozóra való mentés? Mert a helyreállítás enélkül gyakorlatilag lehetetlen. Sőt, ransomware esetén semmilyen garancia nincs arra sem, hogy az esetleges váltságdíj fizetés után valóban kapunk privát kulcsot, és újra hozzáférünk az adatainkhoz: vagy igen, vagy nem. Így akkor marad nekünk a mentés, mint egyetlen hadra fogható módszer, de ezt sem mindegy, hogyan tesszük, ezért most ehhez adunk néhány hasznos tanácsot. Először is azt kell tudni, ha a mentés csupán helyi, azaz ugyanarra az adathordozóra készítjük: legyen az ZIP mentés, backup, local shadowcopy, rendszer-visszaállítás vagy éppen helyi tükrözés, akkor ez nem ér semmit, mert az ilyen kártevő egyszerűen letörölheti, illetve a helyben tárolt tükrözött másolatokat is letitkosítja. Ha már egyszer bejutott a gépünkre egy Cryptolocker, vagy hasonló titkosító kártevő, akkor minden Windows alatt mappelt - értsd felcsatlakoztatott, betűjellel megosztásként hozzárendelt - meghajtónkon is végiglépked a titkosításával, így sajnos az összes bedugott USB tárolónk, hálózati meghajtóink, de még a felhős tárhelyünk is áldozatul eshet. Ez pedig még akkor is így van, ha az adott megosztás nem is Windows alapú gépen található, de onnan elérhető, legyen például Macintosh vagy Linux alatti mappa megosztás.

Mindig győződjünk meg arról, ha a mentésünk készen van, akkor azonnal le legyen választva a tároló eszköz a rendszerről. A fentiek miatt a nap 24 órájában csatlakoztatott külső merevlemez állományai ugyanúgy elvesznek, mint a helyi tartalom. Emellett pedig

készítsünk rendszeresen csak olvasható formátumban - CD, DVD lemezre is. Mind a megírt optikai lemezeket, mind pedig az esetleges külső winchestert érdemes a géptől távol, például egy másik lakásban, tűzbiztos széfben tárolni. Természetesen a kisebb adatkapacitás nehezíti a feladatot, de ennek ellenére hasznos, mert egyelőre olyan vírust, amelyik DVD lemezre írna, egyelőre még nem ismerünk :-). És azt csak zárójelben jegyezzük meg, a mentést titkosítani is érdemes, hiszen ha egyedül csak azt lopnák el, akkor is veszteséget szenvedünk el.

A felhős tárhely is besegíthet a mentésben, mi mindazonáltal itt is a titkosított tárolásban hiszünk, de ezt döntse el mindenki maga. Felhő tárhely esetében kétféleképpen is menthetünk: vagy egy dedikált munkakönyvtárunkat, meghajtónkat szinkronizáljuk vele valós időben, vagy alkalmanként oda is feltöltjük a mentési köteteinket. Számos ilyen felhős alkalmazás nem hagyományos betűjeles megosztásként viselkedik, hanem saját tárolási formátumban dolgozik, így ezek zömével elkerülhető, hogy ott is dúlás, pusztítás legyen. Azt sem szabad elfelejteni, ha beüt egy esetleges fertőzés, azonnal meg kell akadályozni, hogy a sérült adatok felülírassák a korábbi tiszta mentési fájlokat.

Amint említettük, legyen párhuzamosan több különböző verziónk is a mentésből, ne mindig bambán és gépiesen felülírva az előzőt. Ha egyszer kiderül, hogy esetleg mégis bejutott a fertőzés, akkor így nagyobb eséllyel találunk korábbi sértetlen állapotot, lesz miből válogatni a nehéz órákban. Itt végül is ellentmondunk annak a régi szabálynak, hogy ne tároljunk semmit se redundánsan, most éppen pontosan erre van szükség.

Egy jó mentési szisztéma kiválasztása, megtervezése persze hosszabb ideig tart, de mindenképpen érdemes vele foglalkozni, ne legyünk lusták, mert egyre inkább nélkülözhetetlen. Muszáj rendszeresen nem csak inkrementális (egymásra épülő), hanem néha teljes különálló mentéseket is végezni, sőt ezek közül valamilyen logika és ütemezés alapján egyes adathordozókat nem felülírva azokat véglegesen örökre megőrizni. Végül régi vesszőparipánkat is emlegetjük, miszerint csak a kipróbált, visszaállítással is tesztelt mentés nevezhető valódi mentésnek.

- Óvatosság, biztonságtudatosság

Legyünk biztonságtudatosak, vagyis ne kattintsunk ismeretlen feladótól származó gyanús e-mail üzenetek linkjeire, mellékleteire. A felhasználó a leggyengébb láncszem. Ez a biztonságtudatos címke már jó 9-10 éve szerepel a köztudatban. A legkisebb vállalkozásnál ténykedő egyszerű munkavállaló is bedolgozik valahová, ami már kiemelt célpont lehet, aztán a BYOD keretében a tabletünkön, okostelefonunkon számos bizalmas dokumentumot hurcolunk, amiket nem lenne jó ha ellopnának, vagy ha elveszítenénk. A felhasználók biztonsági képzése akkor jó, ha rendszeres, és ebben a megtévesztések (social engineering) módszereknek is szerepelniük kell. Az is fontos, hogy hogyan kerülnek a kártékony kémprogramok a felhasználók gépeire. Nagyon sok esetben felelőtlen kattintással, illetve trójai programok telepítésével.

Olyan védelem, amihez nem kell gondolkodni, nincs

15. fejezet: Mobiltelefon

Kulcsszavak: ismeretlen hívás, külföld, emelt díjas szolgáltatások

Tények: A 18-44 év közötti okostelefonosok 25%-a nem emlékszik az utolsó alkalomra, amikor nem volt vele a mobilja. A mai átlagos okostelefon nagyságrenddel fejlettebb, mint az 1969-es Holdra szállást segítő akkor számítógépes rendszer.

2014-ben három brit vállalatot is megbüntettek amiatt, mert a vizsgálatok szerint különféle Androidos alkalmazásokba olyan rejtett rosszindulatú funkciót rejtettek, amelyek révén az áldozat drága emelt díjas szolgáltatásokra iratkozott fel tudtán kívül. A trójai alkalmazás használata során a jóhiszemű áldozatok bárhova is kattintottak az app képernyőjén, azzal rejtve feliratkoztak felnőtt tartalmakat értékesítő szolgáltatásokra. Az akkori 330 ezer angol fontos bírság mértéke is mutatja, komoly problémáról van szó. Ezzel együtt a felhasználók majdnem fele bankol hordozható okoseszközéről, harmaduk pedig rendszeren elektronikusan vásárol is a segítségével, miközben tévesen úgy vélekedik, hogy szemben a klasszikus számítógéppel okostelefonon vagy tableten semmilyen vírus vagy biztonsági fenyegetés nem érheti.

Mobilos tippek

- Antivírus szoftver feltelepítése itt is ajánlott!
- Csak megbízható alkalmazásokat telepíts!
- PIN kód, képernyő zár - használd őket!
- Kapcsold ki a Geotaget!
- Bluetooth, Infra – Jelszavazd, használat után kapcsold ki!
- Óvatosan a rejtett számokkal!
- Ismeretlen, vagy külföldi számot utasítsd vissza, és ne hívd vissza!
- Nyereményért se add meg a mobilszámodat!
- Ha kéréstlen hívások, vagy SMS-ek jönnek, szólj egy felnőttnek!

No platform is safe - ez az állítás teljesen igaz. Vagyis vírusmentes rendszer nem létezik, de természetesen a helyzet különbözik ezeken. Míg a Microsoft Windows alapú gépeken tavalyi adat alapján több, mint 310 millió egyedi kártevő kód létezett, addig ez a szám Macintosh OS X, illetve Linux rendszereken "mindössze" pár százezer. De az utóbbi években meredeken emelkedett például az Androidra készült kártevők mennyisége, így mindenkinek azt javasoljuk, hogy minden platformon használjanak biztonsági megoldást. Android esetén ez még azzal is súlyosbodik, hogy a nevesebb gyártók prémium modelljeit kivéve - Google Nexus, néhány Samsung és LG típus - ritkán vagy sosem kapnak biztonsági frissítéseket, így ezeknél a készülékeknél kizárólag a vírusvédelmi programunkban bízhatunk.

Nem kívánt hirdetések mobilon

Az átlag ingyenes programok is igyekeznek valahogy megélni, cserébe reklámokat jelenítenek meg, amelyek időnként több adatforgalmat generálhatnak, mint összes hasznos netes tevékenységünk, vagy költségoldalon akár több forgalmi díjat fizethetünk,

mintha ha pár dollárért megvettük volna a fizetős változatot. De emellett vannak félreérthető, ijesztő reklámokkal operáló módszerek is, egy ilyenről lesz most szó. Átlagos esetben persze annak is van egyfajta bája és varázsa, ha mondjuk pókeroldalakat vagy sportfogadást ajánlgatnak, de a hamis riasztás, a vírusokkal kapcsolatos felugrók szerintünk nem etikusak, már egyáltalán nem tartoznak a "még belefér" kategóriába. Például találkozhatunk olyannal, amely olyan magyar nyelvű átverős üzeneteket jelenít meg, mint: "(1) Új vírust észleltünk". Hogy hol észlelték és kik ezek a "mi", az sosem derül ki egyértelműen, és ugye akkor ahhoz, hogy többet tudjunk, kattintani kellene. Az egyik csalás esetén az volt olvasható a kijelzőn: "Androidja vírusos lehet. Az antivírus frissítésére lehet szükség. Javasolt lépések: 1. Adja meg mobilszámát a visszaigazolásához 2. Távolítsa el az összes vírust és védje meg a készülékét. Futtasson egy keresést és távolítsa el a vírusokat azonnal". Telefonszámot megadni, kattintani azonban nem érdemes. Ugyanis nem arról van szó, hogy valaki vagy valami e percben vírusosnak látja a gépünket, hanem ez egy reklám képernyő, egy ajánlat, ami azért valljuk be, igyekszik megijeszteni, megfélemlíteni a felhasználókat. Aki nekik ugyanazokat a kérdéseket kellene feltenniük, mint a hagyományos PC esetében a felugró ablakban jelentkező hamis antivírusok esetében. Hogyan választunk antivírust: a felugró ablakost negligáljuk, inkább mi keressük a megfelelő alkalmazást, utánanézzünk a tudásának, teszteredményeinek, a fejlesztők weblapjának, supportnak, fórumokat olvasunk, letöltünk ingyenes próbaváltozatot, és aztán az információk birtokában, sürgetés mentesen eldöntjük, hogy bizalmunkat és pénzünket hova helyezzük. A lényeg, ha valaki ilyenkor megadja a mobilszámát és kattint, azzal állítólag szerződést fogad el, és figyelmetlenül egy igencsak húzós árú fizetős szolgáltatásra iratkozik fel. Még ma is lehet SMS-sel vehető csengőhangot kapni, sőt ezeket reklámozni a tévében. Például az említett ajánlat is ehhez hasonló volt, annak aki elfogadta és nem olvasta el alaposan az apró betűs részt, 15 EUR-ba - kb. 4400 HUF - került rendszeresen HETENTE. Ami a valódi, a Google Play piacon kapható fizetős legális antivírusok teljes éves díjánál is magasabb összeg.

A Hacking Team RCSAndroid kémprogramja az alábbi tevékenységekre képes: képernyőmentést és fényképet is tud készíteni, monitorozza a vágólapot, ellopható vele a wifi hotspotok és online fiókok jelszava, beleértve a Skype, Facebook, Twitter, Google, Whatsapp, Mail és LinkedIn jelszavakat is, mikrofonnal bármit fel lehet venni, a beépített médiaszerver szolgáltatással a telefonhívásokat is, ellophatók az sms-ek és e-mailek, nyomon követhető a telefon lemásolhatók a névjegyek. Az RCSAndroid kódját 2012. óta aktívan használták, de az informatikai biztonsággal foglalkozó kutatók csak 2014-ben találtak rá és leplezték le. Kétféle módszerrel fertőzték meg a készülékeket: vagy küldtek egy szöveges üzenetet az áldozatnak, amiben egy fertőzött weboldalra csábították őket, illetve készítettek egy BeNews nevű appot is, amit a hivatalos Android Play Áruházból bárki le tudott tölteni.

Egy új átverésnél valahonnan megszerzik a telefonszámunkat, majd a bank nevében felhívnak minket azzal a szöveggel, hogy bankkártya - csalás áldozatai lettünk, és emiatt diktáljuk be a PIN kódunkat, és azt ígérik, hamarosan futár érkezik a bankkártyánkért, hogy azt megvizsgálhassák és letilthassák. Ha valaki van annyira naiv, hogy mindezt elhiszi, akkor kisvártatva ténylegesen érkezik egy "futár" a bankkártyáért, majd kártya és a PIN

birtokában pénzt vesznek fel vagy vásárolnak a kártyánkkal. A telefonszámunkhoz pedig könnyen hozzá lehet jutni. Már a 2013-as év is gigantikus feltörések és adatszivárgások éve volt, az Adobe, a Target áruházlánc után jött az eBay, Michaels Stores, Egészségügyi minisztérium - Montana, Snapchat, Neuman Marcus, Texas St. Joseph Health System, AOL Mail, Yahoo Mail, Coca-Cola Company, Deltek Software Developer, University of Maryland, U.S. Veterans of Foreign Wars - de a sor a végtelenségig folytatható lenne, és bár nevesítve nincs, biztosan számos magyarországi szivárgás is történt. Ilyenkor nem csak eladhatják a feketepiacon, rossz kezekben kerülhet a személyes adat, de sokszor a PasteBin és más hasonló fórumokon nyilvánosságra is hozzák. Ezek birtokában pedig sokkal könnyebb testre-szabott támadást indítani: felhívni, nevén szólítani, bediktálni neki a saját címét és ezzel elaltatni a gyanakvást.

Mit tehetünk azért, hogy ne jussanak hozzá túl könnyen a számunkhoz? Minden ellen nincs orvosság - de azt azért megtehetjük, hogy a közösségi oldalon nem plakátoljuk ki publikusan a lakcímünket, telefonszámunkat, nem adunk ezzel magas labdát. Nem is ez a fő kérdés egyébként - mert barátaink feltört számítógépéből, vagy ellopott telefonjából is megszerezhetők ezek az információk. A lényeg inkább az ilyen esetleges hívások kezelése. Ne higgyünk el mindent, igazoltassuk a hívó felet, és azonnal fogjunk gyanút ha személyes adataink után érdeklődik vagy bediktált linkre kéri, hogy kattintsunk. A biztonságtudatosság, és az egészséges gyanakvás (paranoia) az elsődleges megoldás. Kijelenthetjük, hogy a tájékozottság kulcsfontosságú, hiszen ha tudjuk, hogy például a bank sosem küld futárt a bankkártyánkért, akkor már nem is fogunk ennek bedőlni.

16. fejezet: Mobileszközök - okostelefon, tablet

Kulcsszavak: trójai, lopás elleni védelem, kill switch, jailbreak, szülői felügyelet

Tények: Mivel az emberek elkezdtek tömegesen mobilon bankolni, ezért meredeken növekszik a mobilos banki trójaiak száma. Egy 2015-ös kimutatás szerint már több mint 22 ezer ilyen programot tartanak számon. A szabályok szerint 2015. július 1. után Kalifornia államban már kizárólag csak olyan telefont lehet értékesíteni, amelyben alapértelmezetten engedélyezett állapotban tartalmazza a lopásgátló Kill Switch opciót. Korábban azokban a városokban, ahol a Kill Switch technológiát tesztelték, drasztikusan, 20-40%-kal csökkent a mobil lopások száma.

A ComScore 2016-os "U.S. Cross-Platform Future in Focus" című, az internethasználók körében végzett felmérés adatai szerint már jóval több időt töltünk a mobiljainkkal, mint asztali számítógépeinkkel. Az adatok alapján az látható, hogy az online eltöltött idő nagyját, 65%-át már a mobilok adják.

A Dekra nevű baleseti elemzésekkel foglalkozó német cég 6 európai főváros 14 ezer gyalogosának részvételével végzett kutatásának eredményéből az derült ki, hogy a stockholmiak 23.6%-a gyaloglás közben is a mobilját nyomkodja. Üzeneteket gépelnek, zenét hallgatnak vagy telefonálnak, illetve sokan mindezt egyszerre teszik.

Védeni kell az eszközeinket

Egy 2012-es kutatás szerint már akkoriban is az internet felhasználók 36%-a az okostelefonjával kapcsolódott a világhálózathoz, 19%-uk alapkészülékével érte el a netet és 10%-uk használt tabletet. Azóta ezek a mobilitási arányok még hangsúlyosabbak lettek. A számítógépek biztonsága, a vírusok elleni védekezés mindennapjaink részévé vált, senkit nem kell már meggyőzni a fontosságáról. Ugyanakkor egyre többször olvassuk leveleinket, dokumentumainkat okostelefonon, s közben eszünkbe sem jut, hogy adataink ugyanolyan veszélyben lehetnek, mint egy védelem nélküli számítógépen. Egy korszerű mobil biztonsági termékében olyan megoldásoknak kell helyet kapni, mint a proaktív védelem, SMS/MMS Antispam, hívásblokkolási lehetőség, biztonsági audit, lopás elleni védelem, illetve védelem jogosulatlan biztonsági telepítések ellen. A lopásvédelem esetén például üzenhetünk a beépített kamera által amúgy is lefényképezett tolvajnak vagy ha hamar észbe kapunk, bekapcsolhatunk a készüléken egy vijjogó szirénát, de rendelkezésünkre áll a GPS lokalizáció, a SIM kártya figyelés, a készülék távoli lezárása, illetve végső esetben a távoli adat törlés is.

Egy 2016-os magyar felmérés válaszaiból az derült ki, hogy a megkérdezettek 18%-a hagyta már el személyes adatokat is tartalmazó eszközét, amely végül biztonságban megkerült. Nem volt ilyen szerencsés az a 15%, amelynek sohasem került meg eszköze, így csak bizakodni tud abban, hogy nem kerültek illetéktelen kezébe a személyes adatai. Az elhagyott eszközök mellett, a válaszadók 20 százaléka talált már más által elhagyott adathordozót és nagy többségük meg is nyitotta ezek tartalmát (az összes válaszadó 18 százaléka). Hasonló eredményt mutat az ESET egy közelmúltban végzett angliai felmérése

is. A 22 ezer darab kabátokban, zakókban felejtett eszközök mindössze 45%-a jutott vissza eredeti gazdájához, a maradék körülbelül tízezer pendrive és a rajtuk lévő adatok sorsa mindenki számára ismeretlen.

Mit jelent ez a Kill Switch a gyakorlatban? Azt, hogy mostantól aki telefont vesz, ott már default opció, hogy ez be legyen kapcsolva. Ha ellopják a telefonunkat és bejelentjük, akkor a szolgáltató azonnal elvégez rajta egy távoli adattörlést (remote wipe), ezt követően pedig kizárólag egy egyedi azonosítóval lehet a készüléket újra működésre bírni, még factory reset esetén is csak ezzel a kóddal kapcsol be a telefon.

Nyilván lesznek majd, akik bebizonyítják, hogy ez sem 100 %-ig feltörhetetlen - ahogy semmi ne az - mégis ez egy kiemelkedően hatékony fegyver lehet a mobil tolvajok ellen. Még érdemes pár szót szólni az "alapértelmezett állapotról". Nyilván azért lényeges, hogy aki nem ért ehhez, nem telefonguru, azt is hatékony megvédje. A lopásoknál ugyanis ha alaphelyzetben bekapcsolt Kill Switch mód szerepel, akkor ez már védi nagy többséget, még akkor is, ha az úgynevezett "átlagfelhasználó" jó eséllyel nem is érti mi ez az egész, vagy fordított helyzetben egyszerűen elfelejtheti, ha neki kellene kézzel egyedileg bekapcsolni. Mindezek a fejlesztések (Find My iPhone, Activation Lock) az iOS7 esetében már most is, de az Android Lollipop 5.1 készülékek esetén is nagyban segíthetnek majd visszaszorítani a bűnözést.

2012-ben az úgynevezett USSD (Unstructured Supplementary Service Data) biztonsági hibák veszélybe sodorták az Androidos készülékeket. Az USSD kódok (a kódok csillag (*) karakterrel kezdődnek, majd kettős kereszttel (#) vagy számokkal folytatódnak, melyekhez parancsok vagy adatok tartoznak, és a végét is egy kettős kereszt zárja) eredeti célja, hogy a távközlési szolgáltatók távolról is támogatni tudják a telefonkészülékeket. Ilyen kód például az IMEI szám lekérdezése, vagy a telefonok gyári beállításainak visszaállításához használt kód is. Viszont ha ilyen aktivitásokat kezdeményeznénk a telefonunkon, akkor ez lehetővé teszi a kiberbűnözőknek, hogy távolról töröljenek adatokat a telefonkészülékekről, például úgy, hogy a felhasználót egy URL címre irányítják, akár közvetlenül, akár egy egyszerű szöveges üzenettel vagy QR kód használatával. Erre aztán az antivírus gyártók elkészítettek egy olyan alkalmazást, amellyel védekezni tudunk. Például az ESET USSD Control a Google Play áruházból ingyenesen letölthető megoldása gyanús telefonszámokat USSD (Unstructured Supplementary Service Data) kódjuk alapján kiszűri és ellenőrzi még mielőtt az okostelefon tárcsázója hívná azokat, és minden rosszindulatúnak látszó USSD kód felfedezésekor figyelmeztet és blokkolja a parancs végrehajtását. Azóta ez a védelmet már beleintegrálták a mobil védelmi alkalmazásba, így ezt is tartalmazza a mobil vírusvédelmi Mobile Security csomag.

Androidos telefonokra - ez a rendszer uralja jelenleg a piac legnagyobb szeletét - kis odafigyeléssel elkerülhetjük a hamis, kémkedő, vagy "hazatelefonáló" kártékony alkalmazásokat, ha az alábbi dolgokra ügyelünk:

- Vigyázzunk, ha egy várva várt app túl korán megérkezik. Ez is lehet egy intő jel, hiszen a bűnözők mindig figyelemmel kísérik az aktuális megjelenéseket. Különösen a nagyon várt

programokra koncentrálnak, ezért nem lehet meglepetés, hogy például a BlackBerry Instant Messenger azonnali üzenő alkalmazást már sokan várták. Így történhetett meg az, hogy egy nem működő hamis "BlackBerry Messenger for Android" megjelenése mégis 100,000 letöltést generált, az óvatlan letöltők pedig szerencsétlen módon egy adware-rel, azaz kényszerű reklám programmal lettek gazdagabbak.

- Alaposan nézzük meg, miből használunk "free" változatot. Ez a free kérdés nem is olyan egyszerű, elég ha csak arra az aspektusára gondolunk, hogy az ingyenes, de cserébe reklámokat megjelenítő appok a hálózati forgalmunk, illetve akku üzemidőnk jelentős részét, vagy akár nagyobbik részét is kitehetik. Ezenfelül a freemium kategória bizonyos esetekben tud igen sokba is kerülni ;-). Na most mindezeket leszámítva jöhet még a képbe az a forgatókönyv, hogy a kiberbűnözők az átlagfelhasználók számára népszerű alkalmazások - mint például a prediktív gépelésünket "megtanuló" Swiftkey alkalmazás ingyenes változata gyorsan feltűnt a kalóz oldalak kínálatában is, ám a begépelésen és testreszabáson felül egy billentyűzet naplózó kémprogramot is telepített.

- Az adott alkalmazás Androidra hivatalosan nem is létezik. Mégis rábukkanunk egy nem hivatalos letöltési oldalon. Ilyen többször is előfordult már, például az FTL: Faster Than Light PC játék esetében, amely viszont ráadásul a Google Play kínálatában bukkant fel. A Facebookos "előre lájkolás" átveréshez hasonlóan itt is már előre, vagyis látatlanban kellett minősíteni még a letöltés előtt, így a név mellett később megjelent sok csillagos minősítés itt kamu volt. Az FTL fejlesztői egyébként nem terveztek Androidos verziót, a Google pedig gyorsan eltávolította kínálatából a hamis alkalmazást. Egy másik ilyen csalárd eset volt a UPC távrögzítő sztori. Eredetileg ez egy hasznos lehetőség, ha nem vagyunk otthon a settopboxtól kartávolságra, akkor is beprogramozhatjuk kedvenc műsorunkat, akár PC, akár okostelefon segítségével. A hiba csak ott volt, hogy ez egyedül iOS-hoz készült el, Androidra nem, ám a túl szép, hogy igaz legyen sokakat megtévesztett. Mégis megjelent egy magyar nyelvű UPC Távrögzítő alkalmazás szintén a hivatalos Marketen, ám hogy hányan töltötték le a letiltásig, és mit tett pontosan, arról nincsenek pontos információink.

- A Google Play a legbiztosabb forrás, ám ez még nem garancia. Bár időnként a Google Play esetén is becsúsznak kártékony alkalmazások, a többi alternatív helyszínhez, store-hoz képest itt lepleződnek le a leghamarabb. A hamis alkalmazások jelentős része kínai áruházakból, vagy kalóz oldalakról származik, ám fontos tudni, hogy a Google Play kizárólagos használata sem garancia a sérthetetlenségre. A szoftver letöltés és használat egy bizalmi kérdés. Ahogy számítógépeink esetében közvetlenül a gyártótól, fejlesztőtől a legjobb letölteni, okostelefon esetében a nagy, jelentős áruházak nyújtják a viszonylag nagyobb biztonságot. Bár sok kínai, és egyéb kalóz oldal kínálja a neves programok szabadon letölthető APK változatát, és teszi ki közben ezekre az "ellenőrzött" címkét, ám ennek valóságtartalma rendszerint igencsak megkérdőjelezhető. Ezért is fontos valamilyen biztonsági, vírusvédelmi programot használni az okoseszközön. Már 2012-ben demonstrálták azt, hogy egy felkészült támadó milyen egyszerűen képes az eredetileg ártalmatlan programot, későbbi frissítéseivel észrevétlenül mindenféle ártalmas részekkel kibővíteni. Szóval itt is előfordulnak hamis, vagy trójai programok, ezért előtte

informálódjunk. Ahogy az e-Bay esetében is megnézzük, ki az eladó, milyen visszajelzéseket kapott, mióta tag, itt is jó előre járjuk körbe a fejlesztőket, nézzük meg az értékeléseket, véleményeket még a telepítés előtt.

- A jó appból is lehet rossz app. Sajnos a sláger, jó nevű alkalmazásoknak, játékoknak rendre megjelennek kártékony hasonmásaik. Az androidos piacteret előzőnlötték a Flappy Cupido, Flappy Plane, Fly Birdie, Ironpants, Angry Birds és hasonló nevű hasonmások. Mind a Google, mind pedig az Apple deklaráltan harcot hirdetett az olyan kétes alkalmazások ellen, amelyek nyilvánvaló klónjai más korábbi híres és sikeres játékoknak, illetve amik egyértelműen a felhasználók megtévesztésére, becsapására íródnak. De mi is vigyázzunk, és figyeljünk oda a fejlesztők valódi kilétére.

- Olvassuk el az engedélyeket. Vegyük a fáradságot, és olvassuk el, mire kér engedélyt a telepíteni kívánt app. Ha túl kíváncsi, és a működéséhez józan ésszel végiggondolva egyáltalán nem szükséges - pl. SMS küldés, címjegyzékhez hozzáférés, fizetős hívások önálló indítása, és hasonló felhatalmazásokat is szeretne, inkább álljunk el az installtól, és keressünk alternatívát. Ám ha a felhasználó figyelmetlenül maga engedélyezi, akkor nincs miért csodálkoznia, ha aztán borsos árú SMS küldés van, de azért ez persze nem ilyen egyszerű, mert az engedélyek terén az alkalmazások eléggé el vannak szállva, és szinte alaptól mindegyik kér mindent - tisztelet a kivételnek.

- Értékelések: nem égbolt vagy tábornoki váll-lap ez. A csillagok mellett mindig olvassuk el a szóbeli értékeléseket is. Amint említettük, van néhány átverős alkalmazás, amelyik a letöltés feltételeként előre kéri a jó minősítést, ám akit becsaptak, rendszerint mérgében kiosztja az appot és figyelmezteti a későbbi érkezőket, hogy ők már ne menjenek lépre.

- Android 4.2-től már mi is ellenőrizhetünk. A telepítés ismeretlen forrásból opció egyébként ésszel és odafigyeléssel bekapcsolható, sőt bizonyos esetekben elkerülhetetlen is, például ha éppen biztonsági mentésből állítjuk vissza az alkalmazásainkat, akkor ehhez ideiglenesen engedélyezni kell. A későbbi 4.2 Android változatban pedig bevezetésre került egy újdonság, a Biztonsági beállítások között az úgynevezett "Verify apps" vagyis alkalmazás ellenőrzési lehetőség, amelyet bekapcsolva figyelmeztetéseket kaphatunk, amennyiben kártékony program telepítését indítanánk el.

Időközben jelentek meg a piacon szülői felügyelet programok is Android platformra. Az egyik ilyen lehetséges védelem az ESET Parental Control for Android, melynek segítségével a szülők ellenőrizhetik, hogy gyermekeik telefonjaikon milyen weboldalt nyitnak meg, milyen alkalmazásokkal játszanak, vagy akár rugalmasan beavatkozhatnak, hogy letiltsák azokhoz a hozzáférést. A program barátságos módon elmagyarázza a gyermekeknek, hogy melyek azok az internetes oldalak és androidos alkalmazások, amelyeket biztonságosan használhatnak, megnyithatnak. Az ilyen alkalmazás lehetővé teszi, hogy a szülők bármikor ellenőrizhessék gyermekeik tartózkodási helyét, és olyan üzeneteket küldhessenek nekik, amelyeket a gyermekeknek el kell olvasniuk és vissza kell igazolniuk ahhoz, hogy tovább használhassák az eszközüket.

17. fejezet: Játék, játékkonzolok, okos tévé

Kulcsszavak: chat, online játék, korhatár, xbox, playstation, nintendo

Tények: A korhatár jelzések nem csak a televíziós és mozi műsornál van jelen, hanem a játékszoftvereknél is. Azonban ezt sok esetben teljesen figyelmen kívül hagyják nem csak a gyerekek, de a szülők is.

Egy átlagos amerikai gyerek, mire felnő 100 ezer gyilkosságot lát a televízióban. Meg kell tanulnia megkülönböztetnie a valóságot a fikciótól. A "borzalom" képeit is megkapja: film, videó, internet formájában - ilyen korábban több száz évig nem volt. A vizuális információ azonban erős inger, emiatt ez nagyon romboló. A virtuális közegben az erőszakos (verekedős, zombis, stb.) játékoknak az az üzenete, hogy "nézd milyen ügyesen gyilkolsz".

A gyerekek manapság igen korán kezdik a kütyük és a net használatát. Egyes felmérések szerint negyedük már 2 és 5 éves kora közt okostelefonnal, és asztali gépen Flash játékokkal játszik. Hogyan tarthatjuk biztonságban gyermekünket netezés, vagy online játék közben? A "sehogy" válasz túl általános volna, persze valóban nem egyszerű a helyzet, de azért lehet hasznos lépéseket tenni az ügy érdekében úgy, hogy közben mégse kelljen naphosszat a válla fölött a képernyőjét ellenőrizni.

Mindig legyünk tisztában azzal, hogy melyik kütyü megy éppen online

Az online játékoknál gyakori a beépített csetelési lehetőség, ám ezeken is előfordulhat zaklatás, vagy trágár beszéd. Brit felmérés szerint az ottani szülőknek csak 16%-ban tisztában azzal, hogy például egy Xbox vagy a Nintendo DS konzol esetében is van lehetőség bizonyos szülői felügyeletre, illetve az életkornak megfelelő korlátozások bevezetésére. A klasszikus PC-n már lényegesen jobb arányokat látunk ugyanerre, ott 46%-ban használnak valamilyen szülői felügyeleti megoldást.

Helytelen hozzáállás

Sajnos a helytelen szülő hozzáállásból is nagyon sokat látni. Sok esetben éppen a szülő veszi meg/engedi meg az erőszakos, 18 karikás játékokat a kiskorúak pl. GTA V., Resident Evil, stb. A konzolos játékkínálatot nézve az embernek néha az az érzés, mintha a játékok 80%-a zombis, gyilkolás lenne. Az erőszakos játékok hatására nézve nincsenek egyértelmű mellette-ellene kutatási eredmények, azonban az életkornak nem megfelelő ijesztő tartalmak biztosan kártékonyak. Amint azt Dömös Zsuzsna írta, mindegy, hogy zombi vagy mutáns, a monitoron látott fenyegetésre ugyanúgy reagál a testünk, mint a valós élet veszedelmeire - sőt a félelem egy idő után megszokható, akár csak a drog.

2013-ban egy brit informatikus észrevette, hogy a LG okostévéje látszólag személyre szabott reklámokat jelenít meg. Megpróbálta megkeresni az információgyűjtésért felelős opciót, amit meg is talált, ez az LG Smart AD, amiről addig nem is tudta, hogy egyáltalán létezik. Ám - és most jön a dolog érdekesebb része - miután ezt kikapcsolta, a készülék továbbra is ugyanúgy viselkedett, utána is érzékelte a tévénézési szokásokat, és közben küldte kifelé az adatokat. Ez azért már mellbevágóbb, és valószínűleg kevesen szeretnék,

hogy a testre szabott reklámok érkezzenek, sem pedig azt, hogy például a bedugott USB kulcsok tartalmáról egy ilyen eszköz valahova kifelé jelentsen. Valahol természetes elvárásnak kellene lennie, ha már az élet területén nem érthetünk mindenhez, az adott szakterületek gyártói, szerelői, szakemberei titokban ne éljenek vissza a tudásukkal, ne csapjanak be minket.

A dolgok internete (Internet of Things, IoT) sokféle biztonsági felvetést fog még a felszínre hozni, de egyetlen példát most beidézünk. Ha valakinek modern, hangvezérlésű Samsung okostévéje van, akkor érdemes a felhasználói licencszerződés (EULA) alábbi passzusát komolyan venni: „Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.”. Magyarul bizalmas információkról ne beszéljünk a televízió közelében, mert a hangfelismerő rendszer a felvett hangot továbbíthatja külső szerverek felé.

Érdemes végezetül pár szót ejteni úgy általánosságban is a játékokról. Manapság egyáltalán nem szokatlan, hogy már a gyerekjátékok is tartalmaznak elektronikát, kamerát, hangfelvevőt vagy éppen valamilyen egyszerű számítógépes modult. 1999-ben például a gyermekek egyik kedvenc játékszere, a válaszoló szőrös Furby baba volt. A beszédet rögzítő, majd azt visszajátszó játékszerek olyan hangokat, zajokat, beszélgetéseket, információkat rögzíthetnek, amelyek rossz kezekbe kerülve - elveszve, ellopva, szervizben, kidobva - kellemetlenségeket okozhatnak nekünk, vagy családtagjainknak. Az már csak járulékos esemény, hogy a Furby baba emellett áldozatul esett a biztonságos repüléssel kapcsolatos szabályozásnak is. A Szövetségi Légügyi Hatóság véleménye szerint 10 ezer láb magasságban a Furby babáknak kötelezően kikapcsolt állapotban kellett lenniük, illetve ki kellett venni belőlük az elemeket, nehogy megzavarhassák a fedélzeti navigációs rendszert. Érdekes módon aztán a technikai fejlődés ezt a területet sem hagyta parlagon, például a 2012. után megjelenő újabb Furby változatok például már egy mobil alkalmazás segítségével egy másik Furby babával is képesek lettek kommunikálni. Mindenesetre ezt is érdemes végiggondolni, amikor biztonságos otthonunk és környezetünk kialakításán töprengünk.

2015-ben fedeztek fel azt a legújabb számítógépes kártevőt, amelyik a Full Tilt Poker, illetve a PokerStars online játékaiban kémkedik, és menet közben képernyőképeket készít a játékosok lapjairól, amiket elküld a támadóknak, akiknek innentől már áll zászló a nyereségről van szó. Ez a kártevő célzottan a két legnagyobb online póker oldal, a PokerStars és a Full Tilt Poker ellen irányult. A Win32/Spy.Odlanor trójaiként azonosított kártékony kódot legtöbbször maguk a felhasználók telepítik a gépükre olyan pókerrel kapcsolatos fertőzött segédprogramokkal, mint pókerjátékos adatbázisok, póker kalkulátorok, (Tournament Shark, Poker Calculator Pro Smart Buddy, Poker Office), stb. Illetve a biztonsági kutatók fertőzött trójai változatokat találtak olyan általános segédprogramokból is, mint például a Daemon Tools és uTorrent. Működése közben a trójai folyamatosan kommunikál a támadók C&C vezérlő szerverével, és az összegyűjtött adatokat - képernyőképeket, ellopott jelszavakat - elküldi. Felfedezésekor a kártevő főként Oroszországban és Ukrajnában terjedt, de emellett a Cseh Köztársaságban,

Lengyelországban és Magyarországon is találtak több áldozatot. Az nem derült ki egyértelműen, hogy a kártevő készítői a lopott adatok birtokában manuálisan játszottak a játékkal, vagy pedig valamilyen automatizált botnetes módon.

18. fejezet: Függőség, szenvedélybetegségek

Kulcsszavak: mértékletesség, játékszenvedély

Tények: A videojáték is komoly szenvedélybetegséggé fajulhat. 2012. márciusában egy tajvani fiatalember annyit játszott, hogy belehalt. A 23 éves játékfüggő Chen Rongyou nonstop netkávézóban halt meg, és a személyzet csak 8-9 óra múlva vette észre, hogy már nem él. 2014 júliusában egy kínai házaspár két gyermekét is eladta, hogy a pénzből online játékokat vásárolhassanak. 2010-ben börtönbe került egy koreai pár, akinek a gyereke éhen halt, amíg szüleik az online játékba belefelejtkeztek. A 3 hónapos Kim Sa-rang alultápláltságban halt meg 2009. szeptemberében, mialatt szülei, Kim Jae-beom és élettársa részt vettek egy 12 órás maratoni Prius Online nevű 3-D fantasy játékban. Bár a kislány 2.9 kg-mal született, de halálakor már mindössze 2.5 kg volt a testtömege. A 2014-es esztendőben hozzávetőlegesen 19 ezren haltak meg opioidos (heroin) fájdalomcsillapítók szedése miatt az Egyesült Államokban. Ez az összes ottani 47 ezer túladagolós haláleset 40%-a, ami közel ötszörös növekedést jelent tizenöt év alatt, illetve nagyjából duplája a heroin miatt elhunyt áldozatok számának. Egy ezzel kapcsolatos felmérés szerint tízből amerikaiból négy ismer fájdalomcsillapító-függőt, minden ötödik embernek pedig a saját családtagja érintett a problémában. Egy 2016-os felmérés (University of Pittsburgh School of Medicine) szerint minél gyakrabban látogatja valaki a Facebookot és társait, annál nagyobb valószínűséggel lesz depressziós. A felmérést 1787 amerikai részvételével végezték, akik átlagosan napi 61 percet töltöttek a közösségi oldalakon, lehetett megállapítani depresszióra utaló jeleket. Egy 2016-os kutatás szerint (Innocent Drinks, 2016.) a felnőtt brit lakosság nagyjából ötöde okostelefon-függő. Átlagosan naponta 2 óra 13 percnyi időt (heti 16 óra) tölt okostelefonja vagy tabletje nyomkodásával, a fiatalabbaknál pedig ezek az arányok még rosszabbak. A britek 46%-a átlagosan 15 percenként legalább egyszer előveszi és megnézi a kijelzőt, sőt általában a mellékhelyiségbe is magukkal viszik a kütyüket. Az egy órás vagy hosszabb kihagyás vagy távollét pedig már észlelhető frusztrációt okoz náluk. A WHO legfrissebb adatai szerint a fiatalok körében az öngyilkosság a harmadik leggyakoribb halálozási ok. A megelőzés szempontjából nagyon fontos lenne, hogy az iskolákban is kellőképpen odafigyeljenek a diákok lelki egészségére.

A közösségi oldalak használata életkortól függetlenül a napi rutin részévé vált, nem ritkán naponta több órát is eltöltenek vele az emberek. Azt, hogy a rászánt időmennyiséget tudatosan fordítják-e rá, vagy csak ott ülve nem, vagy csak alig képesek abbahagyni, arról azért vannak sejtéseink - nagyjából hasonló lehet az effektus, mint amikor valaki érdekes műsor híján sem „képes” kikapcsolni a televíziót, helyette folyamatosan pásztázza a csatornákat, akár órákon keresztül kapcsolgatva köztük. Janni Anikó közösségi oldaláról szóló egyik cikke érdekes felmérésről számolt be. "A kutatócsoport 1787 embert kérdezett meg az Egyesült Államokban a 19-32 éves korosztályból. A kérdőív a közösségi média használati szokásokra koncentrált, az ebből született válaszokat pedig összehangolták a depresszió értékelési eszközeivel. Az eredményekből kiderül, hogy a megkérdezettek átlagosan 61 percet használják naponta a felületeket, hetente pedig legalább 30

alkalommal látogatják meg a különböző közösségi média fiókokat. Riasztó adat, hogy a résztvevők több mint egynegyedénél megfigyelhetőek voltak a depresszió jelei. A közösségi médiát gyakran használóknál 2.7-szeres a valószínűsége a depressziónak. Aki szinte egész nap ezeken a felületeken tölti az idejét, annál 1.7-szeres a depresszió kockázata."

Itt még a függőség kapcsán érdemes kitérni a szenvedély betegségekkel kapcsolatos egyéb vetületekre.

„Néhány éve egy nagyszabású amerikai kutatás azt az eredményt hozta, hogy miközben a tizennyolcadik életévüket betöltött férfiak körében kétszerese volt a kémiai szerfüggőség aránya, mint az azonos korú nők körében, addig a 12-17 éves korosztályban megközelítőleg azonos az előfordulás. Magyar eredmények arra utalnak, hogy a középiskolás korosztályban a fiúk nagyobb valószínűséggel kísérleteznek illegális szerek kipróbálásával, míg a lányok a legális szerek felé fordulnak. Magyar középiskolások körében olyan adatok születtek, melyek szerint a lányok nagyobb valószínűséggel próbáltak ki valamilyen gyógyszert visszaélészerűen, mint a fiúk, felnőtt populációban is gyakoribb ez a szerválasztás a nők körében. Ez az a szercsoport, ami kapcsán általában a nők veszik át a vezetést, egyéb pszichoaktív szerek tekintetében a férfiak kisebb-nagyobb előnnyel többnyire nagyobb arányszámokat produkálnak."

Napi maximum 2-3 óra játék tekinthető normális mértékűnek, de fontos, hogy a gyermek akkor se hanyagolja el a többi fizikai élethez kapcsolódó feladatát, a tanulást, barátait.

Az internet eltereli a figyelmet, a felmérések szerint maximum 10-15 percet képesek a középiskolások egyhuzamban odafigyelni.

Mit csinálunk a váratlanul felszabaduló, struktúra nélküli szabadidővel? Amikor nincs feladat, nem kell reagálni. A többség már szinte állandóan a mobilját nyomkodja. Mikro idő, így nevezte Rab Árpád az előadásában, amikor agyunknak kellene a szünet, a csend, hogy elgondolkodjunk, pihenjünk, lazítsunk, odafigyelhessünk a jelen pillanatra.

Egy 2016-os brit felmérés azt mutatta ki, hogy Angliában a gyerekek alig töltenek időt a szabad levegőn. A parkban, játszótéren, erdőben, a természetben a megkérdezett 5-12 éves gyermek közül 64% egy óránál kevesebbet tölt naponta. A 2000 gyerek részvételével történt vizsgálat eredménye szerint 20% semennyi időt sem tölt szabadterben, 10% pedig legalább egy éve nem járt erdőben, nemzeti parkban, úgy egyáltalán a természetben. A szomorú eredmények okai között valószínűleg az elektronikus kütyükkel való foglalatosság, és a TV képernyő előtti üldögélés is előkelő helyet foglal el. Emellett az is elgondolkodtató, hogy az angol gyerekek ezzel kevesebb időt töltenek a szabadban, mint a börtönben a kötelezően előírt szabadtéri tartózkodás révén az elítélt rabok.

Önértékelési zavarok

Mindenki a legjobb pillanatait teszi ki, ahogy Tari Annamária erről szóló előadásának címe igen kifejező: „Isteni szelfik – a tükörbe inkább nem nézek... Online boldogságparádé... A

tartalom fejezetben már szó esett általánosságban arról, hogy vannak a neten hamis, nem igaz információk is. Sokan a közösségi oldalakon is szépítik, felnagyítják a kedvező oldalukat, a kedvező történeteket. Ezeknek persze lehet örülni, de semmiképpen frusztráljon bennünket, ne ássa alá önértékelésünket.

Idézet egy cikkből, ahol ilyen „bezzeg mások” típusú jellemző címeket soroltak:

"Bezzeg a Facebook-os ismerőseim mind olyan szerelmesek és boldogok."

"Mennyit utazgatnak és milyen menő helyeken járnak. Egy csomót edzenek, mindenki csitti-fitti, én meg csak itt tespedek."

"Jesszusom, ez a csaj még mindig milyen jól néz ki! Egy ránc sincs rajta... én meg lassan úgy nézek ki, mint egy leharcolt shar pei."

"Anyám, micsoda étel-költemények! Hogy ennek még ilyenekre is van ideje, hogy így tálaljon, én meg jó, ha kiveszem a rendelt kaját a dobozból..."

Ezzel kapcsolatban a helyes gondolkodás, hozzáállás is segít, valamint ne váljunk rabjává, megszállottjává a mások életét figyelgető, napi akár több órák időtartamra is a közösségi oldalak olvasgatásának. Soha ekkora rálátásunk nem volt még - az internetnek és különösen a közösségi hálózatoknak köszönhetően - mások életére, mindennapjaikra. Hogy aztán ezek a megörökített pillanatok, beszámolók mennyire valóságosak vagy megszépítettek, az egy másik kérdés. Probléma akkor keletkezik, ha összehasonlításokat teszünk a saját életünk, eredményeink, javaink, mindennapjaink és másokéi közé. Ez még a felnőttektől is higgadt önmérsékletet, stabil értékítéletet, kellő mértékű önbecsülést kíván, hogy ezeket mint érdekességeket éljük meg, nem pedig frusztrációként.

Mire figyeljünk, mik lehetnek a függőség (addikció) jelei?

Ha valaki szinte minden idejét az interneten tölti, és elhanyagolja a valódi életbeli dolgait: emberi kapcsolatok, barátok, tanulás, kötelezettségek, kommunikáció, társas lét, szabadidő programok, akkor ez a virtuális életének a túlzott formája. Ugyancsak kóros tünet lehet, ha valaki dühkitöréssel, türelmetlenséggel, ingerültséggel reagál a berendezések műszaki hibájára vagy weboldalak elérhetetlenségére, játékok hibájára vagy az ebben való vereségre, az internet kapcsolat ideiglenes megszűnésére. Igen jellemző, hogy valaki minden idejében - beleértve a mikroidőnek nevezett pár percek is, sorban álláskor, metrózás alatt, villamosmegállóban való várakozáskor - a kütyüjébe temetkezik, "nyomkod". Sokszor a lázas tevékenység mindössze az e-mailek sokadszori ellenőrzése, facebookozás, instagramos képek böngészése, vagy játék.

Puskás Pálma Index portálon megjelent cikkében 7 jelet említ, amiből a játék, illetve a net függőség kiderül:

- „1. Egész nap a játékra gondolok.
2. Egyre több és több időt töltök játékkal.
3. Azért játszom, hogy megfeleljek a valóságról.

4. *A környezetemben élők megpróbálták visszafogni ezt a szokásomat, sikertelenül.*
5. *Rosszul érzem magam, ha nem játszhatok.*
6. *Veszekszem a családommal vagy a barátaimmal a játékkal töltött idő miatt.*
7. *Elhanyagolok más, fontos dolgokat (iskola, munka, sport), csak, hogy játszhaszak.”*

Érdemes megfigyelni az utcán, mennyien végeznek ilyen kényszercselekvéseket. Az online lét, és a közösségi oldalak idejében nem csak gyereknél, de a felnőtteknél is megfigyelhető, hogy túlságosan kitárulkozóak: nevüket, címüket, minden tevékenységüket, étkezésüket fotókkal dokumentálják. Ez nem csak olyan időpocséklás, ami ráadásul keveseket fog érdekelni, továbbá túlságosan sok információt adunk magunknak betörőknek, rosszindulatú embereknek, hanem kényszeres szokássá is válhat. Ezek időben való észlelésében, megelőzésében nagyon szerepel van a családnak, amibe persze a megfelelő szülői példamutatás is beletartozik. Az a gyerek, akinek a szülei minden buszon, villamoson a telefonjukat nyomkodják, órákig böngészik a bulvár híreket, állandóan vicces képeket, videókat néznek és osztanak meg tömegesen, nem várhatják el, hogy gyerekük másképp viselkedjen. A családi programok, közös kirándulás, beszélgetés elől sose vegye el az időt a gépezés. Jó ötlet lehet például, ha közös egyezség alapján a közös étkezések "kütyümentesen" zajlanak, vagyis ekkor se a gyerek, se a felnőtt ne vigye az étkező asztalhoz a telefonját, tabletét, laptopját.

19. fejezet: Kihez fordulhatunk

Kulcsszavak: *kék-vonal, jelentem gomb, segítségkérés*

Tények: *Trevor Foulk a Floridai Egyetem PhD kutatója 2015-ben kísérletet végzett a negatív viselkedéssel kapcsolatban. Ha valaki negatív viselkedés áldozata vagy tanúja lesz, akaratlanul is aktiválódnak benne az erre érzékeny receptorok, és ezután a kétes érzelmi töltetű viselkedést is inkább negatívan értékeli. Eszerint az ilyen típusú viselkedésformák mintegy betegségként képesek terjedni például munkahelyi szervezetekben. Foulk és kollégái rámutattak a negatív viselkedés veszélyeire: a szemtanú éppen úgy válhat terjesztővé, ahogy nagy valószínűséggel megfertőződhet az, aki influenzás beteg után fogja meg az ajtókilincset. Mint a „valódi” betegségeknel, a szándékosság itt sem szükséges, a fertőzés pedig napokig is eltarthat. A nehéz sorsú gyerekeket rendszeresen segítő Ökumenikus Segélyszervezet 2016-ban egy iskolai felmérést végzett a kapcsolati erőszak témájában. Ennek keretében 1100 középiskolás diákot kérdeztek ki, válaszaikból pedig a következők derültek ki: "a tanulók 8%-a látta már a szüleit verekedni, 14 %-uk úgy érzi, hogy nem figyelnek rá, 20% szerint rendszeresen gúnyolják, szidják otthon; 8% pedig úgy érzi, hogy nem szeretik a szülei. Megdöbbentő adatok érkeztek a szakiskolákból és szakközépiskolákból is, volt olyan intézmény, ahol a tanulók 50 százaléka csak aludni járt haza, mert utálta az otthoni légkört."*

Vírusirtó, kékvonal, biztonság tudatosság

Az UNICEF elkészített egy ingyenes magyar nyelvű Help App nevű alkalmazást, amely iPhone, Android és Windows platformra is elérhető. Segítségével olyan információkról olvashatnak, amelyek segítenek nekik megérteni, ha a környezetükben vagy velük szemben támadás, zaklatás, bántalmazás történik. Az ilyen esetekre tanácsokat is kapnak, hogyan kezeljék az ilyen eseteket, hol kaphatnak segítséget. Többek közt az ingyenes Kék Vonal telefonos, chat és e-mail elérhetőségeit is tartalmazza, amelyeket anonim, azaz névtelen módon is igénybe tudnak venni. A Nemzetközi Gyermekmentő által üzemeltetett Kék Vonal hívásait szakképzett gyermekjogászok, pszichológusok, gyermekvédelmi szakemberek fogadják, akik képesek segíteni azoknak a gyerekeknek, akik sokszor senkinek nem merik elmondani a problémájukat, vagy tévesen magukat okolják az elszenvedett sérelmeikért. A programot a hivatalos mobil piacterekről lehet letölteni: Android eseten a Play Áruházból, iOS esetén a App Store segítségével, míg Windows alapú mobil készüléknél pedig Windows Phone Áruház polcain találjuk meg a Help APP-ot.

Tájékoztatás:

- A Nemzetközi Gyermekmentő szolgálat áll a Safer Internet program mögött, és évek óta üzemeltetik a Kék vonal nevű segélyvonalat, amit telefonon, chaten, e-mailek keresztül - akár anonim módon is - elérhetnek a gyermekek. Itt szakképzett gyermekvédelmisek, tapasztalt pszichológusok állnak rendelkezésre. Persze ismétlem, ez is roppant fontos, de a megelőzés, az ismeretek átadása akár már első osztálytól kezdődően az igazi megoldás,

és nem maradhat ki a szülők és a pedagógusok képzése sem - mindhárom szereplőnek fontos, tudja, értse, és hajlandó legyen megtanulni a hatásos védekezést. Gyerekeinkből lesznek a jövő munkavállalói is, akik jó esetben már korán megtanulhatják, hogyan maradhatnak biztonságban.

A neten keresztüli megfélemlítés, zaklatás sajnos nagyon gyakori, erre is fel kell készíteni. El kell neki mondani, hogy ilyen időnként bizony előfordul, és a spamekhez hasonlóan itt sem szabad válaszolni a feladónak, a zaklatónak. Ehelyett blokkoljuk vagy tiltsuk le az illetőt, beszéljük meg gyermekünkkel az esetet, durva esetben készítsünk képernyőképet, vagy nyomtassuk ki bizonyítéknak, tegyünk feljelentést a rendőrségen. Emellett a gyerek viselkedésére is oda kell figyelni, ahogy a gyermekek szexuális zaklatása esetén is megfigyelhető tipikus magatartásbeli változás, például gyakori ágybavizelés. Itt is árulkodó jel lehet a váratlanul megváltozott viselkedés, zavartság, félelem esetén okvetlenül kérdezzünk rá, és beszéljük meg. Iskolás korban például az iskolai bántalmazásokról, vagy egyéb megalázásokról készített és internetre töltött képek, videók okozhatnak komoly lelki problémákat, ezek egy kis részénél - inkább külföldön - sajnos öngyilkosság is többször előfordult már.

Tanácsadás, „segítő beszélgetés”:

- Kék vonal alapítvány telefon (kek-vonal.hu)
116-111, 0-24-ig
- Kék vonal alapítvány chat (chat.kek-vonal.hu)
14:00-21:20

Káros vagy illegális tartalmak bejelentése a www.biztonsagosinternet.hu, illetve a NAIH honlapon lehetséges: <http://naih.hu>, valamint az ugyfelszolgalat@naih.hu e-mail címen

20. fejezet: Tudatos szülői hozzáállás

Kulcsszavak: Digitális szülő, élethosszig tanulás

Tények: A felnőttnek a számítógép, az internet jobb esetben csak eszköz a céljaihoz. A gyerekeknek a számítógép, az internet, és a közösségi háló fontos: ÉLETTÉR.

"A Nominet cég felmérése szerint a szülők egyenként átlagosan 208 képet osztanak meg évente kisgyerekeikről. Ezzel pedig már akkor egy hatalmas digitális lábnyomot készítenek számukra, amikor ők még nem is dönthetnek arról, hogy szeretnék-e viselni annak következményeit. A szülők ötöde ráadásul sose ellenőrzi megosztás előtt, hogy nyilvánosan posztolja-e a képet. Nagy részük azzal sincs tisztában, hogy a közzétett kép többé már nem a saját tulajdonuk, és a közösségi oldal azokat engedély nélkül felhasználhatja."

A jó és a rossz szülőt az különbözteti meg egymástól, hogy ha egyáltalán felteszi magának azt a kérdést, hogy ő vajon jó szülő-e, akkor a válasz igen.

A biztonság tudatos hozzáállás sokaknak elég szokatlan, hiszen a hozzáállásunkat, gondolkodásmódunkat kell kibővíteni új lehetőségekkel, mik történtek a nagyvilágban, milyen veszélyek fenyegetnek, ha nem vigyázunk. Csak egy gondolat kíséret: Ha valakinek feltörik az autóját, és megnézik a GPS-t, a mentett útvonalak közt ott valószínűleg lesz a lakcíme. A tolvajnak legtöbbször elég odahajtani, és a kocsiban sokszor ott van a kapunyitó, garázsnyitó a kesztyűtartóban. Néhány lakásba pedig a garázson keresztül is be lehet jutni. Sokan azonban minden sosem gondolják az ilyet végig, pedig a gyenge pontokat mindig lehet találni annak, aki azokat tudatosan keresi. Általában a kényelemszeretet és a tudatlanság a biztonság legnagyobb ellensége. És nincs ez másként a számítógépes környezetben sem.

Az életkornak megfelelő tartalom: nagyon fontos, ebbe beletartozik a TV műsor, az internet, de a vásárolt játékprogram is. Általában a szülők ugyan tudják, hogy fontos a gyermekük online biztonsága, ám jó részük sajnos mégsem hozza szóba sem rendszeresen, sem alkalomszerűen az internetes élet szabályait. A hozzáállás része az is, hogy akkor védhetjük meg, ha rendszeresen beszélgetünk vele az online életéről is.

A modern kori embernek is megvannak a saját problémái, a lelki eredetű betegségek közül az evészavarok, illetve az egyre erősebb környezeti ingerek miatti hamis testképpel kapcsolatos szorongások. A gyermekek esetében is megtaláljuk ezeket, és ha már az interneten talált tartalmakról ennyit beszéltünk, erről is muszáj szót ejteni. A reklámokban mindig mosolygó, fiatal, egészséges, karcsú és izmos embereket látunk, amelyek egy bizonyos fokig hathatnak inspirálóan is, de a "mindenkinek ilyennek kell lennie" üzenet hamis illúzió. A nagyobb gyerekekre jellemző, hogy önértékelési zavarral küzdenek, és míg kifelé kíméletlen kritikával illetnek mindig apró, általuk hibának tartott jelenségek, aközben magukat nem tudják reálisan értékelni, illetve a külső bírálatokra, észrevételekre érzékenyen reagálnak: vagy túlzott agresszivitással, vagy pedig belső összeomlással, depresszióval. Ehhez nyilván az is hozzájárul, hogy folyamatos versenyhelyzetben élnek,

és a közösségi oldalak miatti fokozott kitárulkozás révén szinte igényükké válik a sűrű, gyors és azonnali külső visszajelzés: lájk függők lesznek, illetve hangulatuk a kapott pozitív vagy negatív visszajelzések miatt szélsőségesen ingadozhat a két véglet, a minden rendben és a minden rossz között. A testkép zavar jellemzően inkább lányoknál fordul elő: a külsővel való teljes azonosulás, önbizalomhiány, kóros soványság, illetve anorexia formájában.

Incidens esetén ne hallgassanak

Ha erőszakos, félelemkeltő, pedofil, idegengyűlöletet keltő, terroristagyanús, kártékony, jogsértő, drogfogyasztásra buzdító tartalomba ütköznek, jelentsék a <http://internethotline.hu>, biztonsagosinternet.hu oldalon.

Együttműködés az ORFK-val

Rendszeresen jelentenek be zaklatásokat gyerek és felnőtt esetek is egyaránt előfordulnak.

Volt például egy olyan fórum oldal, amelyet a gyerekek is látogattak, és teljes részletességű használati útmutatásokat közöltek öngyilkosságokhoz. Ezt a bejelentés és a tartalomszolgáltató felszólítása után 2 órával törölték.

A szülői felelősség igen fontos elem, enélkül a többi fél erőfeszítése alig ér valamit. Ebben pedig kulcsszerepet játszik a szülői mintaadás, a tudatos médiafogyasztás. Ha a gyerek azt látja, hogy a felnőtt minden szabadidejét a TV vagy a számítógép előtt tölti, akkor ezt teszi el mintának, mondjunk neki bármit is. Míg ha jut idő egymásra, offline programokra - kirándulás, közös étkezések, sportolás, élő találkozás barátokkal, stb. - és a kiválasztott műsorokat (on demand) nézik a szülők, nem pedig himnuszról himnuszig mindent, akkor annak sokkal nagyobb hatása lesz a gyerekekre.

Vannak veszélyek az interneten, de erre nem a teljes tiltás a megfelelő eszköz. A totális tiltásra van is kedvenc történet, ismerős szülők békeszeretői, békepártiak, akik emiatt aztán tudatosan és pedánsan véletlenül sem vesznek évek óta a gyereküknek játékfegyvert, ez tabu. Aztán eljön egy soron következő születésnap gyereksúr az osztálytársaknál, ahol aztán a vendégségben a gyerekük egész álló este csak a puskával akar lőni, meg a pisztollyal, aknát vet, és gránátot robbant - visszaleng az inga. Ugyanígy nem válik be hosszú távon, ha nem engedjük internetezni, mert akkor ellenőrzés nélkül majd az iskolában, vagy a barátainál teszi ezt, és nem fog róla beszámolni. Tanítsuk türelmesen, ne ijesszük el, de azért a tipikus lehetőségekre: pedofilok, zaklatók, ijesztő tartalmak valamilyen mértékben készítsük fel, hiszen az egészséges veszélyérzetre szükség van. Például ha egyedül keres autós, kamionos, repülő, stb. flash játékokat, és önállóan próbálgatja ezeket, de ha eközben kattintás után valamilyen ijesztő dolgot lát a képernyőn, akkor azonnal szóljon nekünk. Ha ilyenkor kérdez, mindig legyen időnk válaszolni, segíteni, tanácsot adni, odamenni vagy ott lenni vele. Természetesen a mérték, a napi gép előtt eltölthető idő is legyen valamilyen szabályozva.

Ha elmagyarázzuk neki mindig az életkorának megfelelően, mit látott-tapasztalt a virtuális térben, rendszeresen megbeszéljük vele az ott történeteket, ezzel tehetünk a legtöbbet.

Ezek a beszélgetések - kezdve az átverős spamektől egészen a miért hamis a pornófilmekből megismert szexualitás témáig mind segíthetnek kialakítani nem csak a szülő-gyerek közötti kölcsönös bizalmat, de az egészséges kritikai érzéket is a gyerekekben. Fontos, hogy jogukban áll hibázni, és ekkor ne szidjuk le őket, hanem magyarázzuk meg nekik, miben hibáztak és hogyan lehet legközelebb jobban kezelni vagy elkerülni a hasonló helyzeteket. Abban is érdemes megegyezni a gyermekkel, hogy a nevét, címét, telefonszámát és fotót csak a szülő beleegyezésével tegyen fel.

Bár ennek a könyvnek nem témája a szexuális felvilágosítás, nemzetközi kutatásokból jól látszik, hogy a vélt vagy valós érettség, illetve az érdeklődés kezdete egyre fiatalabb korban kezdődik. Kiegészítve ezt azzal, hogy a médiában - televízió, utcai reklámok, újságok, internet - a meztelenség, és a pornográf anyagok mindenki számára könnyen és ingyenesen elérhető közelségbe kerültek. Emiatt fontos az ilyen jellegű gyerek-szülő beszélgetés is, amely a látott vagy olvasott ijesztő, furcsa információkat segíthet tisztázni, és azt is igyekszik megmagyarázni, hogy a pornófilmekben gyakran látható jelenetek nem csak megrendezettek, hanem köszönő viszonyban sincsenek az egészséges párkapcsolatban egymás tiszteletén, szeretetén alapuló intim viszonynak, a nők valós elvárásainak.

Tehát a "mit tehetnek a szülők" kérdésre nem lehet egy mondatos sablonválasszal felelni. A szakemberek szerint az egyértelműen nem segít, ha például a szülők de facto megtiltják gyermeküknek például a Facebook regisztrációt, hanem sokkal hasznosabb engedni és megbeszélni a szabályokat. A tiltás mindig kontraproduktív, és ha például már minden osztálytársának van (néha persze csak trükkösen, hiszen 13 év alatt elvileg valós életkorral nem is lehetne regisztrálni), akkor aki kimarad, az nem akar "lúzer" lenni. Ez pedig egy nagy mozgatóerő a gyereknél, hiszen nem akarnak kimaradni az osztálytársak "flow"-jából. A teljes tiltással egyébként pont azt érik el, hogy később ne velük beszélje majd meg az online életét, ezt pedig a szülőknek kell világosan megérteni. A nagy tiltások után viszont ha titokban mégis megy a Snapchatre, Ask-FM-r, Tumblr-re és hasonlókra, amikről a szülők sokszor azt sem tudják mi az, akkor pedig ezzel teljesen kikerülhet a látókörükből.

Mindegy hogyan éltek a szülők régen, a gyerek nem akar a múltban élni, neki az itt és mostban, ebben az internetes kütyüvilágban, közegben kell okosan és szeretettel segíteni. Hiszen nekik már a számítógép, az internet nem eszköz, hanem élettér. A jó oktatásoknak - amit már első osztálytól érdemes tartani - például éppen az a lényege, hogy a gyerekeknek megmutassa, a saját tudásuk a védelem. Ha vannak minták, lefektetett szabályok, akkor sokkal jobban működhet ez. Ha megbeszélik, hogy például ha valamit fel akar tölteni, előtte kérdezzen; a lakásról sose töltsön fel képet; ha nyaralni mennek, ne jelezze előre; vagy ha valaki ismerősnek akarja jelölni, visszaigazolás előtt kérdezze meg előbb a szüleit, stb.

Emellett a szülőknek is muszáj volna megtanulni, hogyan segíthetnek okosan a gyereküknek. És nekik is meg kellene barátkozni az élethosszig való tanulással, tanulni, érdeklődni, ha valódi segítő partnerek akarnak lenni, maradni. Kisebb gyermekek esetén még hasznos lehet, ha szűrőszoftver, illetve valamilyen gyermekfelügyeleti program

segítségével szűrik, ellenőrzik illetve szabályozzák az internetes kapcsolatot, ám az ilyen szűrő program hatékonysága maximum 8-10 éves korig ér valamit, hiszen utána már kikapcsolhatja, megkerülheti, vagy az osztálytársakhoz átmenve, mobilnetről bármit elérhet, ott már nem lehet tiltani, ám sérülni ott is tud.

Emiatt idővel át kell vegye a szűrés helyét a megelőzés, a "saját tudásod a hatékony védelem" elve, vagyis a biztonságos internethasználattal kapcsolatos tudás elsajátítása. Ha így döntök ez történhet, ha úgy döntök az történhet, ha bajban vagyok ide fordulhatok, ha a barátom van bajban, akkor hogyan segíthetek, stb. Ezért inkább ezeket az ismereteket kell minden gyereknek átadni, megmutatni a lehetséges veszélyeket, és a szülőkkel pedig az online életet rendszeresen megbeszélni. Ha pedig a gyerek időnként mégis hibázik, nem durván leszidni, vagy teljesen eltiltani kell, különben végleg bezárkózik, hanem türelmesen és szeretettel megmagyarázni, pontosan mi volt a hiba, és hogyan lehet ezt máskor jobban csinálni. Egy biztos, ez nem egyszerű feladat, de más út nincs.

„A gravitáció nem ismerete nem mentesít a zuhanás alól.” A szülőnek is folyamatosan tanulnia kell. Sose adjuk fel azzal, hogy mi úgyis kevesebbet értünk a géphez, mint a gyerek, és akkor erre hivatkozva nem csinálunk semmit. Mi is tanulhatunk a gyerekünkötől, és felelős szülőként pedig tanulnunk kell a számítógépes szituációkból is. Ha kell, beszéljünk erről az iskolában a tanárokkal, vagy kérjünk tanácsot a többi szülőtől.

Állítsunk be külön felhasználói fiókot a gyerekeknek

Persze nagy a kísértés, hogy a család közös Windowsos gépéhez időnként csak úgy odaülve lehessen játszani. A korábbi XP esetében ráadásul ez még azzal is súlyosbítva van, hogy a rendszergazdai jogok alapértelmezetten lehetővé teszik, hogy a böngészés közben begyűjtött kártevők is ilyen módon lefuthassanak. Külön felhasználói fiókokkal viszont okosan testre lehet szabni a lehetőségeket.

Digitális gyerek, digitális tanár, digitális szülő, mind új kihívások. Egy 2015-ös gyermekvédelmi konferencián volt ez a "digitális családfő" kifejezés így nevesítve azzal, hogy sok családban mennyire nagy szükség lenne rá. Ő lenne, aki naprakészen átlátja, és ellátja a biztonsággal, biztonságos használattal kapcsolatos teendőket.

Ehhez pedig nem csak az kell, hogy minél jobban megértsük gyermekeink modern kütyüs-internetes életét, hanem az is, hogy a felnőttek, a szülők hajlandóak legyenek tanulni, megérteni és képben lenni az aktuális veszélyekkel, a hatékony védekezés módszereivel kapcsolatban. Ehhez igyekszünk most pár tippet adni.

Az internet világa folyamatosan fejlődik, az ezzel kapcsolatos ismeretanyag pedig állandóan bővül. Ahogy egyre több eszköz csatlakozik a netre - okosórák, érzékelők, lakásriasztók, okostelefon, tablet, játékkonzol, stb. - úgy lesz egyre bonyolultabb a hatékony védekezés. Amikor már az okoshűtők is spammelnek, ez nem tréfadolog.

A következőkben egy alapszintű lista próbál meg a szülőknél abban segíteni, miket érdemes átnézni-felülvizsgálni rendszeresen, hogy a család tagjai viszonylagos

biztonságban legyenek.

Legyen a digitális élet is része a napi beszélgetéseknek, hasonlóan a "mi volt az iskolában?" "milyen volt az edzés" kérdésekhez hasonlóan beszélgessenek a szülők rendszeresen gyermekükkel, mi történt vele a virtuális térben. Emellett segítsenek nekik megérteni, hogyan lehetnek biztonságban, mikre érdemes figyelni, hiszen a biztonságos internethasználattal kapcsolatos ismeretek elsajátítása fogja megvédeni később az incidensektől. Ha tisztában van azzal, hogy ha így döntök ez történhet, ha úgy döntök az történhet, ha bajban vagyok ide fordulhatok - akkor ezzel egyúttal mintegy felvértezzük új, ismeretlen helyzetekre is.

Ha esetleg a gyerek időnként mégis hibázik, akkor türelmesen és szeretettel kell megmagyarázni, hogy pontosan mi volt a hiba, és hogyan lehet mindezt legközelebb jobban csinálni. Ebből a tanulásból a család minden tagjának ki kell vennie a részét.

Az informatikai higiénia elengedhetetlen része a naprakész vírusirtó mellett az is, hogy az operációs rendszerek, és az alkalmazói szoftverek is rendszeresen karban legyenek tartva. Vagyis a megjelenő hibajavító frissítéseket minél előbb töltsük le és futtassuk is őket.

A foltozatlan biztonsági rések ugyanis lehetőséget biztosítanak arra, hogy a kártékony kódok a sebezhetőségeket kihasználva megfertőzhessék a számítógépünket.

Tartsunk rendet, rendezettséget a média állományaink területén is. Családi fotóink, saját dokumentumaink mellett letöltött zenéink, filmjeink és sorozataink is legyenek valamiféle logikus rendben tárolva. Segíthet ebben például a dátum kezdetű fájl- és mappa nevek, például ha a mai napon készült fényképek egy "20160307_Korfu" folderbe kerülnek, hasonlóan a korábbi és későbbi fotókhoz, könnyű lesz őket később megtalálni. Digitális korunkban ugyanis egyre több, és egyre terjedelmesebb méretű állományt kell kezelnünk, tárolnunk, emiatt érdemes rendet tartani, mielőtt felüti fejét a káosz, és helyhiány.

Esetleges adatvesztés esetén ha nincs rend, úgy gyakran azt sem tudjuk megállapítani, éppen mi vesztetett el. A felesleges állományokat pedig érdemes rendszeresen, és mihamarabb törölni, hiszen ez is egyszerűsíti a képet, emellett tárhelyet is felszabadít.

Legyünk kreatívak a jelszavak használatát illetően. A tapasztalat azt mutatja - többek közt az évi Worst Password lista is - hogy a rövid, bugyuta, sablonos jelszó használat komoly kockázatot jelent arra, hogy illetéktelenek is be tudjanak lépni a nevünkben. Ha ezt még súlyosbítjuk azzal is, hogy egy jelszót több helyszínen is használunk, azzal pedig további kellemetlenségeknek tesszük ki magunkat. Beszéljük meg a családtagokkal, hogy a jelszó szerepe éppen az, hogy titkainkat és magánéletünk másra nem tartozó részleteit óvják az illetéktelenektől.

Egészséges titkai mindenkinek lehetnek, ez teljesen normális igény. A jelszó erősségét értékelő weblapokkal tesztelhetjük is, mennyi idő alatt lehetne feltörni őket, illetve az is jó gondolat, ha szimpla jelszó helyett inkább jelmondatokban gondolkodunk, és a

kétfaktoros azonosítási lehetőségeket is kihasználjuk.

Mentsük rendszeresen saját munkánkat, állományainkat. Mindezt pedig csak a backup folyamat idejére csatolt külső adathordozóra tegyük, hiszen ha egy zsaroló kártevő egyszer már bejutott a gépünkre, akkor minden Windows alatt mappelt - értsd felcsatlakoztatott, betűjellel megosztásként hozzárendelt - meghajtónkon is végiggyalogol a titkosításával, így sajnos az összes bedugott USB tárolónk, hálózati meghajtóink, de még a felhős tárhelyünk is áldozatul eshet. A fizetéstől egyébként szinte minden biztonsági cég óva int, hiszen ezzel csak erősítik és tovább bátorítják az elkövetőket, akik nem Grál lovagok, hanem kőkemény bűnözők, emiatt sajnos az esetek jelentős többségében nem is kapjuk meg a szükséges feloldó kulcsot. A nemzetközi statisztika szerint csak a váltságdíj fizetőknél kb. 5%-a jut végül hozzá.

"Minden szenvedés oka a nemtudás". A szülő felelőssége nagyon nagy. Sokan belecsöppentek az internet világába, és nem tudnak vele mit kezdeni, és így segíteni sem tudnak a gyereküknek, aki azt használja. A szülőnek igenis tudni kell, tanulnia kell, hogy értse ezt a világot, és nézze meg, hogy mit csinál a gyermeke nap mint nap a gép előtt! Érdeklődjön, kérdezzen, figyeljen!

21. fejezet: Tudatos gyermeki hozzáállás

Kulcsszavak: látszatvilág, celebek, 15 perc hírnév mindenkinek jár,

Tények: A gyermekek 93%-a folyamatosan online. A 2014/2015-ös tanévben a magyar általános iskolai tanulók szám 748,500 volt. Az amerikai tinédzserek negyede ébredéstől számítva öt percen belül már belép valamelyik hálózatba. Napi átlag száz szöveges üzenetet küldenek. Nyolcvan százalékuk a telefonjával alszik. Negyvennégy százalékuk az összes élethelyzetben online marad. (Sherry Turkle: *Reclaiming Conversation, The Power of Talk in the Digital Age*, 2015.)

Amerikai kutatók szerint a fogyasztói társadalom, a modern szülői nevelés és az internet együttes hatása miatt az emberek egyre nárcisztikusabbak, egyre önzőbbek. Ha úgy alakul, 3 másodperc alatt posztolja a világnak, ami vele történt. Nagyon kritikus mással, és egyre kevésbé kritikus magával.

Egyre erőszakosabb a legójáték - állapították meg az új-zélandi Canterbury Egyetem kutatói. A szakemberek a legó figurák és készletek változásait vizsgálták 1978 és 2014. Kutatásukból az derült ki, hogy mára a dán cég világhírű legószett játékeinak nagyjából 30%-ában szerepel már valamilyen fegyver is. Emellett a jelenleg forgalomban lévő aktuális katalógusok körülbelül 40%-a tartalmaz valamilyen erőszakos elemet.

A legfontosabb védelem a saját tudásod! Ha csak egyetlen egy szabály lenne: "Ne tégy másokkal olyat, amit nem szeretnél, hogy veled tegyenek!". Vigyázzatok egymásra! Véd meg, ha mást zaklatnak!

Külföldön már évek óta önálló weblapja van az öngyilkosságba menekült áldozatoknak, és a felvilágosító munka ellenére sajnos a helyzet évről évre romlik. Magyarországon is történt már több öngyilkossági kísérlet, ezért mindannyiunknak szerepe van abban, hogy ez ellen tegyünk, és a legjobb, ha megelőzzük. Az olyan iskolákban, ahol a gyerekekre figyelő szabályok és pedagógusok vannak, akik a zéró tolerancia jegyében már a legkisebb, kezdeti erőszakot, zaklatást sem tűrik meg: „áll, no ezt nem, ezt itt nálunk nem lehet” felkiáltással, ott lehet a legjobban elejét venni az események elfajulásának, a durvább incidenseknek. Ha nem kapja meg a gyerek kellő időben a visszajelzést, akkor azt a tanulságot szűri le, hogy a jövőben mindezt bátran megteheti, később már csak a határokat próbálgatja, feszegeti.

Hasznos szabályok:

- Ha valaki chat-en, e-mailben zaklat, ne töröld és ne válaszolj, tedd el a levelet bizonyítéknak!
- Te se zaklass másokat, és ha mást zaklatnak, ne továbbítsd!
- Jelentsd a problémát az üzemeltetőknek, tiltsd le, blokkold a küldőt!
- Szólj róla a barátaidnak, szüleidnek, tanáraidnak!
- Segíts a barátodnak, ha ő kerülne ilyen helyzetbe!
- Szükség esetén fordulj a hatósághoz!
- Vigyázz a jelszavadra, ügyelj a biztonsági beállításaidra!

- A közösség a legjobb visszatartó erő!

Próbáld kimenteni az áldozatot! Online akció előtt beszélj a barátaiddal és kérd ki a véleményüket, tanácsukat! Gondol végig előtte: Megéri? Minden megnyilvánulásod, visszavágásod előtt kétszer is gondold meg, mit teszel, milyen harcba bocsátkozol. Ne konfrontálódj a zaklatóval, ez nem használ, sőt ront a helyzeten.

22. fejezet: Tudatos pedagógusi hozzáállás

Kulcsszavak: *pedagógusképzés, személyes példamutatás, egységes iskolai incidenskezelési útmutató*

Tények: *2015-ös adatok szerint ma még mindig mintegy 200 iskolában egyáltalán nincs internet. Az uniós szinthez képest Magyarországon kevés a rendszergazda az iskolákban, valamint a korszerű digitális taneszközök területén is erős elmaradásunk van. A 2014/2015-ös tanévben az általános iskolai tanulók száma 748,500, a köznevelésben az iskolák száma 10,829, míg a köznevelésben a pedagógusok száma 153,000 volt. Az internetes kapcsolat sokszor kihat a pedagógusok iskolán kívüli szabadidejére is. Igen sok iskolában ugyanis a tanárok már zárt Facebookos csoportban beszélnek meg a diákokkal az iskolai ügyes-bajos dolgokat, ahol előzetes megbeszélés szerint a diákok „bármikor” kérdezhetnek is, amire a megállapodás szerint a tanárnak nem kötelező azonnal válaszolni.*

A gyerekeknél az állandó kütyühasználat következtében gyengül az empátikus készség és az önismeret, érzelmileg fejletlenebbek lesznek, minden szabadidejükben vagy a telefonjukat nyomkodják, vagy arról beszélgetnek, amit azon látnak/láttak. Tanáraik szerint nem néznek beszélgetőpartnerük szemébe, egyre kevésbé kezdeményeznek élő beszélgetés, és barátságaik is inkább csak felületes ismeretségek valódi tartós, erős baráti viszony helyett.

Az információ birtoklása még nem tudás, ha 5 másodperc alatt megkeresi a Google-ban, még nem biztos, hogy érti is. Ez nem tudás, hanem információ. Az internet azt az illúziót szolgáltatja, ha megnéz valaki egy YouTube videót, akkor úgy érzi, ő ezt már "tudja".

Bár a pedagógusok egy része már aktívan használja az internetes médiákat, nekik is folyamatosan tanulniuk kell, hogy megvédhessék a gyerekeket. Átfogó programra volna szükség, hogy egységes szakmai ismereteket lehessen átadni számukra.

A gyermekeknek és a tanároknak is meg kell tanulniuk az internet biztonságos használatát. Ez az ismeret anyag nem csak felhívja a figyelmet a problémákra, hanem védekezési módszereket és lehetőségeket is felvázol. Minden szereplőnek meg kell értenie, hogyan legyen óvatos. Például világszerte rengeteg számítógépes kártevő kukkolja titokban a felhasználókat - köztük lányokat is. Ha megtanulják, hogy a nem letakart kamera veszélyforrás, az például sokat segíthet. De ugyanígy praktikus tudnivaló többek közt a megfelelően erős és egyedi jelszavak választása, a vírusirtó és szülőfelügyeleti program futtatása, a közösségi oldalak felelős használata is. Ha a tanár nem érti a szituációt, segíteni sem tud.

Az oktatás során fontos rámutatni, hogy az internet egy remek dolog, de tisztában kell lenni a veszélyeivel. Az a gyermek, aki tudja, mik történhetnek vele a virtuális térben, tudja, hogy kihez fordulhat, ha bántják, ha felkavaró tartalomba ütközik, ha zaklatják, akkor ezzel felvértezi magát. A saját tudása lesz a legfontosabb védelme. Emellett azt is

szoktuk nekik oktatni, hogy vigyázzanak egymásra, ha épp nem velük történik valami rossz, ne hagyják cserben a barátjukat sem. És ne tegyenek mással olyat, amit nem szeretnének, hogy velük tegyenek.

Emellett egy olyan egységes útmutató is hasznos lehetne az iskolaigazgatók számára, amely a különféle számítógépes zaklatások, visszaélések esetében eligazítást nyújtana, mely ügyekben hogyan kell szabályszerűen eljárni, például milyen súlyosságú ügyek kezelhetők helyben, és melyekben kell már a rendőrséghez, illetve a hatóságokhoz fordulniuk. A tapasztalatok szerint egyetlen iskola sem mentes az incidensektől, ezek súlyossága változó. Az egyszerű más postafiókjában annak jelszavával való belépéstől kezdve az olyan eseteken át, amikor a lányok felveszik a fiúk verekedését, vagy valakinek a megverését és felteszik az internetre, sőt a durvább esetben a mobiltelefonnal készült meztelen képeikkel zsarolják egymást.

Szabályokat és best practice módszereket tanítunk, hogy lássák a döntések-következmények vonalat. Mind három szereplőnek folyamatosan képeznie kell magát - így a gyerekeknek, tanároknak és szülőknek is, és felelősséget kell vállalniuk a helyzetekben. Az a pedagógus, aki például azt követeli meg, hogy a diákok rendszeresen a tanítás elején adják le mobiltelefonjukat és meg sem fordul a fejében, hogy valaki pont emiatt kettő telefont fog magánál hordani, módszerével gyakorlatilag nem ér el semmit. Ha azt várjuk a gyerektől, hogy mindent és élethosszig tanuljon, akkor a korszerű számítógépes és oktatási ismeretektől nem zárkozhat el egyetlen pedagógus sem. Itt is inkább a szabályozott használat lenne az üdvöztető a merev tiltás helyett, illetve ez már messzire vezet, de az oktatásban is használható lenne megfelelő appok, tanterv segítségével, ahogy már van olyan történelem tanár, aki a Minecraft segítségével modellezi a gyerekekkel közösen a középkori várakat, csatahelyszíneket.

Zaklatással kapcsolatos szakirodalom a "zerotolerenciat" és a gyerekkorú osztályközösségen belüli véleményvezér mediátorok képzését is jó eszköznek látja.

Azt is érdemes kiemelni, hogy az online üzeneteket könnyű félreérteni, hiszen nincs szemkontaktus, nem halljuk a hangsúlyokat. Minden esetre folyamatosan őrködni kell a gúnyolódó légkör megelőzésén.

Egy pár szó a trágár beszédéről. Ha valaki nyitott szemmel-füllel közlekedik az utcán, járműveken, azt tapasztalhatja, hogy egyre kisebb korban, és nem csak a fiúk, hanem a lányok is rendkívül trágárul beszélnek. Itt nem káromkodásról van szó - amikor indulatosak, haragosak, mérgesek vagyunk, vagy ha a kezünkre ütöttünk a kalapáccsal - hanem a hétköznapi társalgást szövik át tömegesen a szalonképtelen kifejezések. Freud szerint „a káromkodás civilizációs ugrás volt. Az indulatokat szóban kezdték kifejezni az emberek egymás agyonütése helyett.” Ennek persze örülhetünk, de a kiskorúakat óvni kell a trágár tartalmaktól a neten, illetve meg lehet próbálni ezen a területen is kreatívnak lenni: például az osztályban a „hónap hőse” díjat az kapja, aki nem (vagy csak igen ritkán, nem zavaróan) beszél csúnyán. A filmek, játékok, zenék világa elég vastagon hordoz - általában angolul - trágár tartalmakat, amik elkerülhetetlenül elérnek mindenkihez, de jó

ötlet lehet ennek tompítása, mérséklése a mindennapi használatba engedése helyett. És itt azért van egy olyan aspektus is, ami igen gyakorlati: a csúnya beszéddel könnyű megsérteni másokat, amik aztán elfajulva további agressziót szülnek, zaklatásba torkolhatnak. Vagyis itt is a megelőzés lenne a legjobb fegyver.

És végül a technikai fejlődés is olyan, amit nem hagyhat egy pedagógus figyelmen kívül. Ez nem merülhet ki csak a fenti, számítógéppel, privátszféra védelmével, és az internetes zaklatással kapcsolatos korszerű ismeretekben, és a helyes hozzáállásban, hanem ismernie kell a világban szélesebben zajló innovációs folyamatokat is. Például sokan talán még nem is hallottak arról, hogy létezik úgynevezett "diák vizsgaóra", vagy egyszerűen "csalóóra", amelynek segítségével a dolgozatoknál, vizsgáknál komplett szövegeket lehet rátölteni, és ezt egy gombnyomással előhívni a különben csak egy ártatlan órának látszó karórából. De léteznek emellett csaló golyóstollak és zsebszámológépek is, amelyeket pár ezer forintnyi összegért például az Amazon webáruházból bárki könnyen megrendelhet.

Egyébként nem csak a pedagógusoknak, hanem általában a felnőtteknek is nagyon fontos, hogy nyomon kövessék a változásokat, értsék és ismerjék a lehetőségeiket, hogyan védhetik meg privátszférájukat. Például olyan egyszerű esetben, amikor valaki ruhát vesz egy boltban, de aztán 8 napon belül eláll a vásárlástól, jöhetnek elő adatvédelmi kérdések. Néhány helyen ugyanis ilyenkor a vevő nevét, lakcímét is elkérlik a pénzvisszafizetés feltételeként. Erről viszont azt érdemes megkérdezni, vajon a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról szóló törvényi előírásoknak megfelelően kezelik-e, ám azt is fontos kihangsúlyozni, ha valaki mégsem szeretné megadni a nevét és a címét, erre nem kötelezhetik.

Összegezve nagyon ismeret, rendszeres oktatás, figyelem és élethosszig tanulás szükséges ahhoz, valaki valóban képben legyen, naprakész legyen ezekben a kérdésekben. Ezek nélkül azonban nem csak magunkat, de a gyermekeinket, illetve a tanítás idejére ránk bízott gyerekeket sem tudjuk hatékony megvédeni a veszélyekről, és megtanítani őket az internetes világban való biztonságos közlekedésre.

„Minden társadalom egyetlen reménye a jövő. A jövőbe vetett hit. A jövőt pedig a mai gyerekek jelentik számunkra.”

23. fejezet: Szótár, szómagyarázatok

Adware, magyarul kéretlen reklám program

Reklámot megjelenítő speciális futtatható alkalmazás, elsődleges célja olyan reklámanyag kézbesítése, amely a felhasználó számára váratlanul, illetve kéretlenül érkezik. Sok adware alkalmazás hajt végre nyomkövető funkciókat, éppen ezért sorolják ezeket a fürkésző technológiák közé. Számos felhasználó el szeretné távolítani a gépéről ezeket a kéretlen reklámprogramokat, ha azok kémkednek a szokásaik után, nem kívánják látni az adware által megjelenített reklámokat, illetve zavarja őket a reklámprogramnak a rendszer teljesítményét korlátozó hatása.

BOT

A robot szó rövidített alakja, a bot egy feladatokat automatikusan végrehajtó program. Kezdetben a botokat a UNIX világban alkalmazták a rendszergazdák a rendszeresen elvégzendő, sablonos feladatoknál. Némely bot automatikusan cseveg is a felhasználóval, vagy válaszol a feltett kérdésekre, mintegy utánozva egy valódi, hús-vér embert. A bot rossz célokra is felhasználható: segítségével egy távoli támadó átveheti az irányítást az áldozat megfertőzött számítógépén. A cél pontosan ez: egyetlen gépről fertőzött számítógépek százezerei válnak távirányíthatóvá. A károkozók (botnet azaz botnet pásztor) az eltérített számítógépek erőforrásait kéretlen levélszemét (spam) küldésére, illegális szoftverek letöltésére és tárolására használják. Nem ritkán pornográf anyagok tárolására, illetve különféle számítógépes támadásokban (DoS, DDoS) való részvételre is használják, sőt meghatározott tarifa fejében akár bérbe is adják ezt a kapacitást. A bot ezenfelül képes végigpásztázni az áldozat merevlemezét, és arról bizalmas adatokat továbbít egy távoli weboldalra, és ezekkel a lopott személyes, banki, lakcím, társadalombiztosítási stb. információk segítségével további bűncselekményeket követnek el (identity theft, azaz személyiség lopás). Az ilyen fertőzött gépeket gyakran zombi gépeknek is nevezik.

BOTNET hálózatok

Botnet hálózatnak nevezzük az olyan botokkal fertőzött gépek csoportját, melyeket távolról központilag irányíthat a rosszindulatú támadó. Mostanában a peer-to-peer (P2P) botneteket használják leggyakrabban. Ezeknek a botnet hálózatoknak nincsen a hagyományos értelemben vett vezérlőközpontjuk, mégis valamennyien egy zombi hadsereg részét képezik.

Hoaxok, azaz beugratások

A hoaxok általában ostoba csínyek, amik lánclevelek vagy úgynevezett városi legendák (Urban Legends) formájában terjednek. A computer vírusokról szóló beugratások megpróbálnak félelmet kelteni, bizonytalanságot és kétséget ébreszteni a címzettekben, hogy egy észrevehetetlen vírussal állnak szemben (mitől is lenne észrevehetetlen, ha egyszer észrevevessük). Néhány ilyen levélben valóban volt olyan rosszindulatú kód, amely képes volt fájlokat törölni a felhasználók gépeiről. Az ilyesfajta üzeneteket hagyjuk figyelmen kívül, és egyszerűen töröljük ki őket. Jó szerencsénk az életben semmilyen

módon nem függ attól, hogy egy figyelmeztető levelet elküldünk-e húsz legjobb barátunknak, és ez a módszer semmiképp nem szolgálja gépünk biztonságát, ráadásul felesleges levélforgalmat is okoz.

Malware, magyarul kártevő

A Malware kifejezés a MALicious SoftWARE, azaz a kártékony szoftverek szavak összevonásából keletkezett. Ez a meghatározás lefedi az olyan károkozót, mint például a vírusok, férgek, trójai programok és botok. Tulajdonképpen ez egy általános technikai kategória, amelybe tekintet nélkül mindenfajta károkozó programot be tudunk sorolni.

Payload, magyarul büntető rutin

Kiegészítő funkció, például adatlopás, fájlok törlése, lemez terület felülírása, BIOS felülírása, és ehhez hasonló, melyet a vírusok, férgek, illetve trójai programok tartalmaznak. Fontos megjegyezni, hogy a büntető rutin nem okvetlenül okoz kárt, például a Form.A nevű vírus a hónap egy napján minden billentyű leütésekor zajokat produkál, és ezzel valóban nem károsít semmit. Trójai programok esetében ez a titkos rutin az, amit a programozó eredetileg meg akart valósítani.

Phishing, magyarul adathalászat

A phising (kiejtése hasonló a fishing, vagyis halászat szóhoz) a pszichológiai megtévesztés egy olyan módozata, mellyel csalárd módon bizalmas személyes információkat próbálnak megszerezni: ilyenek például a jelszavak, hitelkártya adatok. Ezt általában úgy valósítják meg, hogy hamis e-mail üzenetet küldenek egy megbízhatónak látszó személytől vagy intézménytől, és ebben a levélben látszólag szabályosan különböző információkat kérnek. A leggyakoribb adathalász támadásoknál közismert, neves bankok nevében jelentkeznek, és speciális szolgáltatást ígérnek, illetve különféle szankciókat helyeznek kilátásba, ha az ügyfél nem követi az utasításokat. Néha ez a levél szinte a megszólalásig hasonlít az eredetire, és olyan céges elemeket jelenít meg, mintha valóban a megjelölt helyről érkezett volna. Általában a levél tartalmaz egy internetes linket is – ez szintén megtévesztésig hasonlít például a hivatkozott pénzügyi intézet eredeti honlapjára – és ha a gyanútlan áldozat rákattint erre a linkre, ott a bűnözők már képesek a hamis űrlapba begépett személyes adatokat „elhalászni”. Fontos megjegyezni, hogy bankok és olyan valós cégek, mint például az E-bay árverési portál vagy a PayPal fizetés közvetítő sosem kérnek be ügyfélnevet és jelszót kényszerű e-mail üzenet útján – ilyenkor legyünk gyanakvóak. Az ilyen hamisított levelek mindig valódinak látszanak, de a levél vége felé rendszerint tartalmaznak egy, a jelszó lopáshoz használható linket is.

Rootkit

A rootkit egy olyan eszköz vagy ezek gyűjteménye, amelynek segítségével titokban lehet egy számítógépet vezérelni. Kezdetben a rootkitek a UNIX operációs rendszerre jelentek meg, (beleértve a Linux platformokat is) és ezek olyan eszközök gyűjteményét jelentették, amely alkalmas arra, hogy egy támadó rendszergazdai jogokat szerezhesen az adott rendszeren belül (ezt hívják a UNIX alatt „root” jognak). A rootkit kifejezést Windows alapú rendszereken általában az olyan programok meghatározására szokták használni, amelyek futó folyamatokat, állományokat vagy rendszerleíró adatbázis (Registry)

kulcsokat rejtenek el az operációs rendszer, illetve a felhasználó elől. Az ilyen Windowsra telepített rootkit olyan funkciókat használ, amellyel nem csak saját magát képes elrejteni, hanem további kártékony kódokat – például billentyűleütés naplózót (keylogger) - is észrevehetetlenné tud így tenni. A rootkitek nem szükségképpen csak rosszindulatú kódok elkészítéséhez használhatók, de az utóbbi időben jelentősen növekvő mértékben használták fel ezt a rejtőzködő technikát a rosszindulatú kódok készítői.

Scams, magyarul internetes csalások

A csalások nagyon hasonlatosak az adathalászathoz, de ilyenkor nem a személyes adataink kifürkészése a támadók célja, hanem emberi érzéseink manipulálására (social engineering) építenek: szánalmat ébresztenek bennünk, vagy kapzsiságunkra alapoznak. Például majdnem minden természeti katasztrófa (földrengés, vihar, áradás, háború, éhínség) után megjelenik a csalási szándék állítólagos jótékony gyűjtések formájában. Van aztán a csalásoknak egy illetékekkel kapcsolatos csoportja (ezeket gyakran 419-es vagy nigériai típusnak is nevezik), amikor a csalók azzal kecsegtetnek, hogy nagy összegű pénzhez juthatunk, ha segítünk egy vagyont kimenekíteni valamilyen afrikai országból. Ezek a trükkök mindig arra épülnek, hogy megkérik az áldozatot, küldjön előlegbe az adminisztrációhoz egy kisebb összeget (ez lehet akár több ezer dollár is). Előfordulhat az is, hogy az adott országba utazó megtévesztett áldozatot egyszerűen elrabolják vagy megölik. A kevésbé szélsőséges csalási esetekben igen sok ember vesztett már el így sok ezer dollárt.

Spyware, magyarul kémprogram

A kémprogram meghatározást kétféle értelemben is használják. A szigorúan vett definíció szerint ez egy nyomkövető program (Tracking Software), amelyet tudtunk és beleegyezésünk nélkül telepítettek a számítógépünkre. A felhasználói szokások kifürkészésével – ez az egyszerű böngészési előzményektől kezdve egészen a bizalmas banki azonosító-jelszavakig terjedhet - ezen adatok egy illetéktelen harmadik félnek való elküldését értjük. Némely kémprogramot egy másik program beépített részeként találhatunk meg (hasonlatosan a trójai alkalmazásokhoz), de lehet számítógépes férgek büntető rutinja is, illetve terjedhet olyan weblapokon keresztül is, amelyeken számítógépes sebezhetőségeket (exploit) használnak ki, hogy csendesen a háttérben telepíthessék fel ezeket a kémeket az áldozatok gépeire. Létezik aztán számos olyan hamisított kémirtó program is, amely éppen maga egy kémprogram. Tágabb értelemben kémprogramokat – az Anti-Spyware Coalition szervezet meghatározása alapján – kémkedő és egyéb kéretlen alkalmazások kategóriába soroljuk. Ez a definíció magában foglal bizonyos süti (cookie) állományokat, kereskedelmi forgalomban kapható billentyűleütés naplózókat és egyéb nyomkövető technológiákat.

Trojan Horse, magyarul trójai faló vagy trójai program

A trójai faló – melynek történetét a görög regékből ismerhetjük – egy olyan program, ami valami mást csinál, mint amit magáról eredetileg állít. Ez a más nem minden esetben okvetlenül romboló vagy káros, de sok esetben igen: fájlokat törölnek, felülírják a merevlemezt, vagy távoli hozzáférést biztosítanak a rendszerhez a támadónak. Klasszikus trójai általában tartalmaz egy billentyűleütés naplózót (keylogger) is, amelyet készítői

játéknak vagy valamilyen hasznos segédprogramnak álcáznak. Az ilyen trójaikat sokféle céllal alkalmazhatják: rejtett távoli (backdoor) elérést szeretnének biztosítani egy adott számítógéphez, ellenőrizni kívánják a billentyűleütéseket, valamint jelszavak lopására specializálódnak (a legtöbb kémprogram ez utóbbi kategóriába esik).

Vírus

A vírus egy olyan program, amely képes reprodukálni saját magát – akár megegyező, akár módosított formában – egy másik végrehajtható kódba. A vírusok többféle gazda programot (hosts) használhatnak, a legismertebbek: végrehajtható állományok (számítógépes programok), betöltő (boot) szektorok, szkript kódok (például a Windows Scripting, vagy a Visual Basic), illetve dokumentumokba ágyazott makró utasítások. Amikor egy vírus beszúrja saját másolatát egy másik végrehajtható kódba, ezzel biztosítja azt, hogy a vírus kódja is lefuthasson, amikor az eredeti program fut, és úgy terjed, hogy futás közben mindig újabb, tiszta és megfertőzhető programok után kutat. Néhány vírus felülírja az eredeti programkódot – tönkretéve ezzel az eredeti programot –, de a legtöbb esetben úgy fűzik hozzá magukat, hogy mind a gazdaprogram, mind a víruskód életképes maradjon. A kódolástól függően a vírusok sokféle fájl típuson keresztül képesek terjedni a rendszerben, hálózati megosztásokon keresztül is, dokumentum állományokban, de akár lemezek rendszerbetöltő (boot) szektoraiban. Bár néhány vírus e-mail üzenet útján is terjed, az elektronikus levelezésben szereplő kártevők legnagyobb része féreg. A vírusnak elegendő, ha a sokszorosításáról megfelelően gondoskodik, nem szükséges, hogy büntető rutint is tartalmazzon vagy hogy széles körben elterjedjen.

Worm, magyarul féreg

A számítógépes terminológia szerint a férgek a vírusok egy részhalmaza, és bár megvan a képességük önmaguk sokszorosítására, a fertőzéshez hordozó gazdaprogramot (host file) nem igényelnek. Ahogy a vírusok programokat fertőznek meg, úgy a férgek rendszereket árasztanak el. Az ilyen férgek rendkívül gyorsan képesek sebezhetőséget tartalmazó hálózatokon terjedni, és ehhez még a felhasználó beavatkozása sem szükséges. A féreg általában fertőzött e-mail üzenetekkel terjed, amelyben valamilyen számítógépes sebezhetőséget kihasználó kód található, és maga a levél valamilyen csábító, érdekes üzenetet közvetít (például Anna Kournikova fotói). A féregket általában sokkal könnyebb eltávolítani, mint a vírusokat, mert nem fertőznek fájlokat, egyszerűen törölhetőek. A féreg rendszerint gondoskodik arról, hogy minden rendszerindításkor lefuthasson, ezt az Indító Pult (Startup Folder) vagy a rendszerleíró adatbázis (Registry) bejegyzések manipulálásával éri el. Jegyezzük meg, a féreg nem szükségképpen okoz rombolást.

selfie:

olyan fotó, amelyet valaki magáról készít, jellemzően okostelefonnal vagy webkamerával, azután pedig feltölti valamelyik közösségi oldalra, vagy képmegosztóra

e-whoring:

Olyan internetes csalási fajta, amikor csálók vetkőző lánynak kiadva magukat pénzt, hitelkártya adatokat gyűjtenek be. Az ígért élő vetkező show helyett előre felvett videót mutatnak a kukkolni vágyó zömmel felnőtt férfi áldozatoknak. A megkárosított áldozatok

szégyenükben általában nem tesznek feljelentést, míg a csalók a pénzlehúzáson kívül sokszor kémprogrammal is megfertőzik a gyanútlan áldozatok számítógépét.

cyberbullying: Magyarul online bántalmazásnak fordíthatjuk. Különbféle bántalmazások, zaklatások, megszégyenítések, kiközösítések tartoznak ebbe a kategóriába, ahol az áldozat a bántalmazások hatására szenved, viselkedése gyökeresen megváltozhat, például nem akar többet iskolába menni, vagy iskolakezddéskor hasfájás, fejfájás és egyéb tüneteket produkál. A nagy nyilvánosság miatt a szégyen nagyon erős lehet, és az internetes online tér miatt mindez sok esetben nem szűnik meg az iskolából hazaérve sem.

grooming: bizalomba férkőzés. Jellemzően az a tevékenység, amikor egy idegen felnőtt digitális úton, például hamis profil segítségével megpróbálja megszerezni a gyermek bizalmát és barátságát azzal a céllal, hogy ezen információkkal később valamilyen formában visszaéljen. Később ennek segítségével pedig megszarolja, például élő találkozást kezdeményez, szexuális visszaélésre veszi rá, stb.

sextorsion:

szexualitással - fotó, videó, információ - kapcsolatos zsarolás

sexting: Sajnos egyre fiatalabb korban fordul elő, hogy a fiatalok saját magukról, vagy társukról hiányos öltözetű vagy részben vagy egészben meztelen fotókat készítenek, és azt elküldik, megosztják másokkal. Még olyan extrém eset is előfordul, hogy nem az egész testükről, hanem csak a nemi szervükről készítenek ilyen fényképeket és küldik el közösségi oldalon üzenetben, telefonon. Fontos tudni, hogy egy ilyen képnek az elküldése - még ha eredetileg csak egy konkrét e-mail címre, telefonszámra vagy egyetlen ismerősnek ment privát üzenetként - után bármikor kikerülhet véletlenül vagy szándékosan a szélesebb körű nyilvánosság elé. Ez pedig rettentően kínos következményekkel járhat: a áldozatot további képekért, pénzért vagy szexuális szolgáltatásokért zsarolhatják cserében azért, hogy a szülei, tanárai ne értesüljenek erről vagy ne ossza meg ezeket a teljes internet nyilvánossága előtt. Számos gyermek öngyilkossága vezethető vissza ilyen felelőtlen tetre. A kikerült képek felett elveszítjük a későbbi ellenőrzést, "az internet nem felejt", és évek, vagy évtizedek múlva is visszatérhetnek ezek másolatai az online térben történő újabb megosztásokban.

Generációk:

A generációs felosztás az alábbi születési évek szerint szokták számítani:

Baby boom.: 1946-1964

X generáció: 1965-1979

Y generáció: 1980-1995 - még felnéz beszélgetés közben

Z generáció: 1996-2004 - beszélgetés közben is nyomkodja a kütyűjét

Alfák.....: 2005- utáni születésűek

A szakirodalmakban a legtöbb helyen kihangsúlyozzák, hogy ez a felosztás pusztán elméleti, a gyakorlatban pedig sosem különülnek el ilyen élesen, sőt olyan véleményekkel is lehet találkozni, amelyek szerint mindez divatjamúlt, túlhangsúlyozott, erőltetett.

chat:

azaz csevegés, ami a Wikipédia klasszikus meghatározása szerint olyan társalgási forma, amely 2 vagy több ember között online - leggyakrabban az interneten keresztül - történik.

PUP:

A Potentially Unwanted Programs rövidítéssel jelölt, magyarul „Kéretlen alkalmazások” olyan programok, amelyek adware-eket (reklámozó modulokat) tartalmaznak vagy felesleges programokat, böngészőbe beépülő toolbar-okat telepítenek a számítógépre.

24. fejezet: A szerző bemutatása, ajánlott weboldalak és szakirodalom

A szerzőről:

Csizmazia-Darab István, IT biztonsági szakértő

Sicontact Kft, antivirus.blog.hu

A számítógéppel való kapcsolata 1979-ben indult, egy évig nagygépes R20 operátorként dolgozott a FÜTI-ben. 1980-tól a Kandó Kálmán Műszaki Főiskola, majd a Hungaroton Stúdiója következett, ahol stúdiós-hangtechnikus volt, és időközben egy saját C64 is bearanyozta a hétköznapijait. 1989-ben szerezte meg a Számalk-ban a programozói diplomát, és a Volán Tefunál helyezkedett el. 1990-től az ERŐTERV-ben folytatta, ahol a dBase, Clipper és C programozással párhuzamosan a vállalat vírusvédelmi felelőse is volt egy 400 gépes hálózatban. 2001-től a 2F Kft.-ben vírusvédelmi tanácsadóként a Kaspersky és F-Secure programokkal foglalkozott, majd 2002-től a Vírus Híradó portál főszerkesztője is lett. 2003-tól a PC World magazinban online szerkesztőként helyezkedett el, majd 2006-tól az IHG-Ramsys Kft.-ben volt szoftverfejlesztő. Ezután a VirusBuster Kft. víruslaboratóriumában vírusanalizáló, sajtóhír-felelősként dolgozott, majd 2007-től lett IT biztonsági szakértő, tanácsadó a magyarországi NOD32 képviselőnél (Sicontact Kft.) - azóta is itt dolgozik.

1988-ban írt először cikket vírusvédelmi témában, 2001 óta pedig rendszeresen jelentek meg írásai a nyomtatott sajtóban, emellett pedig Vírus Híradó portálon is. 2007. óta gazdája az antivirus.blog.hu oldalnak. IT biztonsági témában számos rádió- és TV interjúban szerepelt, valamint konferencia előadóként is rendszeresen szokott felkéréseket kapni. 2014-ben elnyerte az „Év információbiztonsági újságírója” címet.

Munkája során folyamatosan igyekszik szolgálni az IT biztonság népszerűsítését szakszerű, de egyben közérthető és érdekes formában értékelni, kommentálni az aktuális incidenseket, és persze praktikus tanácsokat is adni a védekezéshez. Emellett pedig 2013. óta a Safer Internet előadójaként a gyerekek biztonságos internethasználatra való nevelését is fontos feladatának tartja.

Ajánlott weboldalak:

<http://saferinternet.hu/>

<http://www.webidomar.hu/>

www.baratsagosinternet.hu

<http://www.saferinternet.org/>

<http://stopthinkconnect.org/>

<http://www.koloknet.hu>

<http://biztonsagosinternet.hu> (Magyarországi Tartalomszolgáltatók Egyesülete, MTE)

<http://internethotline.hu> (Nemzeti Média- és Hírközlési Hatóság, NMHH)

<http://www.eset.hu> (Az ESET vírusvédelmi termékeinek magyarországi képviselője)

https://www.eset.hu/otthoni/parental_control_for_android (ESET Parental Control for Android)

<http://www.beszeljrola.hu/>

Ajánlott irodalom:

- Tari Annamária: Y generáció, Z generáció, Ki a fontos: Én vagy Én?
- Kulcs a net világához - A NAIH tanulmánya a gyermekek biztonságos és jogtudatos internethasználatáról, 2013.
- Barbara Coloroso: Zaklatók, áldozatok, szemlélők: az iskolai erőszak
- Postman Neil: The Disappearance of Childhood (1994.) A gyermekkor eltűnése
- Kevin Mitnick: A megtévesztés művészete
- Herbert Schiller: Tudatipar made in U.S.A.
- William Golding: A legyek ura
- Kemény Zsófi: Én még sosem
- Laboda Kornél: MátéPONTindul
- Kalapos Éva: Massza
- Philip Zimbardo: Nincs kapcsolat

Ajánlott film, színdarab:

- Komabázis: Cyberbully színházi előadás
- Öngyilkosok szobája (2011. lengyel film)
- Az osztálytalálkozó (2013. svéd film)
- A taxisofőr (Martin Scorsese, 1976.)

Online cikkek:

<http://444.hu/2013/08/31/barmelyik-tinibol-lehet-sztar-csak-kozben-nemi-eroszakkal-fenyegetik-az-ask-fm-vilaga/>

<http://antivirus.blog.hu/2012/08/27/>

[a_facebook_szerint_a_pedofilok_is_emberek_vicces#comments](#)

<https://www.brightfort.com/eulalyzer.html>

<http://www.origo.hu/techbazis/20151022-horror-felelem-drog-megszokas-agy-emberi-test.html>

<http://mashable.com/2010/05/10/twitter-follow-bug/>

<http://facebookmarketing.hu/2010/05/11/facebook-adatvedelem-hiba/>

<http://eu.techcrunch.com/2010/05/10/joke-about-blowing-something-up-on-twitter-get-arrested/>

<http://youopenbook.org/>

<http://hu-hu.facebook.com/privacy/explanation.php>

<http://www.rabbitblog.hu/2009/09/11/viselkedes-alapu-celzas-behavioral-targeting/>

25. fejezet: Képanyagok

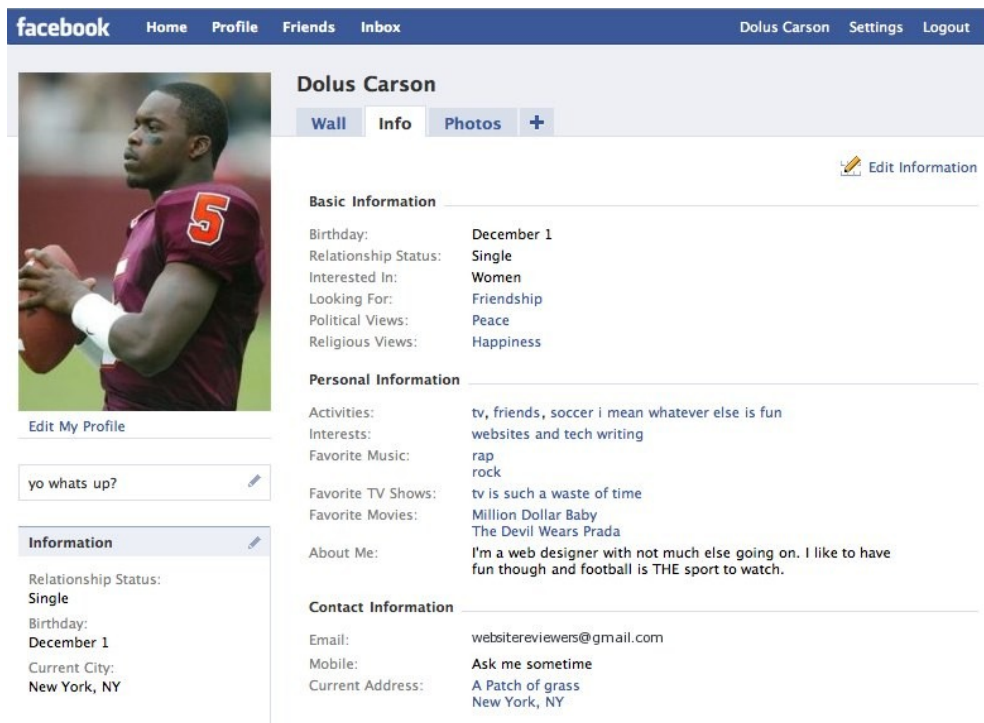
123456	CHARLIE	HELLO	FENDER	GOLF	DONALD	MUFFIN	GIANTS	ROSEBUD	CALVIN
PASSWORD	SUPERMAN	SCOOTER	ANTHONY	BOND007	BIGDADDY	REDSOX	BOOTY	JAGUAR	SHAVED
12345678	ASSHOLE	PLEASE	BLOWME	BEAR	BRONCO	STAR	BLONDE	GREAT	SURFER
1234	FUCKYOU	PORSCHE	FERRARI	TIGER	PENIS	TESTING	FUCKED	COOL	SAMSON
PUSSY	DALLAS	GUITAR	COOKIE	DOCTOR	VOYAGER	SHANNON	GOLDEN	COOPER	KELLY
JESSICA	CHELSEA	CHICKEN	MAVERICK	GATEWAY	RANGERS	MURPHY	0000	1313	PAUL
12345	PANTIES	BLACK	CHICAGO	GATORS	BIRDIE	FRANK	FIRE	SCORPIO	MINE
dragon	PEPPER	DIAMOND	JOSEPH	ANGEL	TROUBLE	HANNAH	SANDRA	MOUNTAIN	KING
QWERTY	AUSTIN	NASCAR	DIABLO	JUNIOR	WHITE	DAVE	POOKIE	MADISON	RACING
696969	WILLIAM	JACKSON	SEXSEX	THX1138	TOPGUN	EAGLE1	PACKERS	987654	5555
mustang	DANIEL	CAMERON	HARDCORE	PORNO	BIGTITS	1111	EINSTEIN	BRAZIL	EAGLE
letmein	GOLFER	654321	666666	BADBOY	BITCHES	MOTHER	DOLPHINS	LAUREN	HENNAI
baseball	SUMMER	COMPUTER	WILLIE	DEBBIE	GREEN	NATHAN	00000	JAPAN	NEWYORK
master	HEATHER	AMANDA	CHRIS	SPIDER	SUPER	RAIDERS	CHEVY	NAKED	LITTLE
michael	YANKEES	WIZARD	PANTHER	MELISSA	GAZWSX	STEVE	WINSTON	SQUIRT	REDWINGS
FOOTBALL	JOSHUA	XXXXXXX	YAMAHA	BOOGER	MAGIC	FOREVER	WARRIOR	STARS	SMITH
SHADOW	MAGGIE	MONEY	JUSTIN	1212	LAKERS	ANGELA	SAMMY	APPLE	STICKY
MONKEY	BITEME	PHOENIX	BANANA	FLYERS	RACHEL	IPER	SLUT	ALEXIS	COCACOLA
ABC123	ENTER	MICKEY	DRIVER	FISH	SLAYER	0V182	8675309	AAAA	animal
PASS	ASHLEY	BAILEY	MARINE	PORNI	SCOTT	JAKE	ZXCVBNM	BONNIE	BRONCOS
fuckme	THUNDER	Knight	ANGELS	MATRIX	2222	LOVERS	NIPPLES	PEACHES	PRIVATE
6969	COWBOY	iceman	FISHING	TEENS	ASDF	SUCKIT	POWER	JASMINE	SKIPPY
JORDAN	SILVER	TIGERS	DAVID	SCOOPY	VIDEO	GREGORY	VICTORIA	KEVIN	MARVIN
HARLEY	RICHARD	PURPLE	MADDOG	JASON	LONDON	BUDDY	ASDFGH	MATT	BLONDES
RANGER	FUCKER	ANDREA	HOOTERS	WALTER	7777	WHATEVER	VAGINA	QWERTYUI	ENJOY
Iwantu	ORANGE	HORNY	WILSON	CUMSHOT	MARLBORO	YOUNG	TOYOTA	DANIELLE	GIRL
JENNIFER	MERLIN	DAKOTA	BUTTHEAD	BOSTON	SKRINIVAS	NICHOLAS	TRAVIS	BEAVER	APOLLO
HUNTER	MICHELLE	000000	FUCKING	BRAVES	INTERNET	LUCKY	HOTDOG	4321	PARKER
FUCK	CORVETTE	PLAYER	CAPTAIN	YANKEE	ACTION	HELPM	PARIS	4128	QWERT
2000	BIGDOG	SUNSHINE	bigdick	LOVER	CARTER	JACKIE	ROCK	SWIMMING	TIME
test	CHEESE	EDWARD	chester	BARNEY	JASPER	MONICA	EXTREME	SHIT	SYDNEY
BATMAN	MATTHEW	CHARLES	Smokey	VICTOR	MONSTER	MIDNIGHT	REDSKINS	SATURN	WOMEN
trustno1	1212	GIRLS	xavier	TUCKER	TERESA	COLLEGE	EROTIC	GEMINI	VOODOO
THOMAS	PATRICK	booboo	steven	PRINCESS	JEREMY	BABY	DIRTY	CASPER	MAGNUM
TIGGER	MARTIN	COFFEE	viking	MERCEDES	111111	CUNT	FORD	STUPID	JUICE
ROBERT	GINGER	xxxxxx	SNOOPY	5150	BILL	BRIAN	FREDDY	SHIT	ABGR1Y4
ACCESS	FREEDOM	bulldog	BIVE	DOGGIE	CRYSTAL	MARK	ARSENAL	GEMINI	77777
LOVE	THOMAS	ncc1701	EAGLES	222222	PETER	STARTREK	ACCESS14	APPLES	DREAMS
buster	GINGER	rabbit	winner	GUNNER	PUSSIES	SIERRA	WOLF	AUGUST	MAXWELL
1234567	BLOWJOB	PEANUT	SAMANTHA	HORNEY	COCK	LEATHER	NIPPLE	3333	MUSIC
SOCCER	NICOLE	JOHN	HOUSE	BUBBA	BEER	232323	ILOVEYOU	CANADA	RUSH2112
HOCKEY	SPARKY	JOHNNY	FLOWER	2112	ROCKET	4444	ALEX	BLAZER	RUSSIA
KILLER	YELLOW	GANDOLF	JACK	FRED	Theman	BEAVIS	FLORIDA	CUMMING	SCORPION
GEORGE	CAMARO	SPANKY	FIREBIRD	JOHNSON	OLIVER	BIGCOCK	ERIC	HUNTING	REBECCA
SEXY	SECRET	WINTER	BUTTER	xxxxxx	PRINCE	HAPPY	LEGEND	Kitty	TESTER
ANDREW	DICK	BRANDY	UNITED	TITS	BEACH	SOPHIE	MOVIE	RAINBOW	MISTRESS
	FALCON	COMPAQ	TURTLE	MEMBER	AMATEUR	LADIES	SUCCESS	112233	PHANTOM
	KILLER	CARLOS	STEELERS	BOOBS	777777	NAUGHTY		ARTHUR	BILLY
	TAYLOR	JAMES	TIFFANY					CREAM	ALBERT
	131313	MIKE	ZXCVBN						6666
	123123	BRANDON	TOMCAT						

500 WORST PASSWORDS

TAKEN FROM PERFECT PASSWORD SELECTION, PROTECTION, AUTHENTICATION BY MARK BURNETT

500rossz.png

Az ötszáz leggyengébb jelszó egy ábrán elhelyezve. A szótáralapú jelszótörések miatt ezeket semmiképpen ne válasszuk, hiszen megfejtésükhöz mindössze másodperc elegendő.



dolus.png

Egy social engineering-kísérlet a Facebookon. Egy hamis profil, nem létező adatokkal, egy élvonalbeli sportoló képét kölcsönözve három nap alatt több mint száz „barátot” eredményezett. Vajon mi járt a kapcsolatként megjelelő emberek fejében? Az biztos nem, hogy mostantól az új „ismerős” akár beláthat a személyes adatlapjukba is

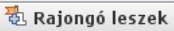


facebook.png

Egy tipikus csali: aki bedől az ilyen állítólagos videónak, az vagy csak a saját gépét fertőzi meg, vagy kompromittált fiókja nevében ráadásként még ismerőseit megbombázza

hasonló üzenetekkel.

facebook Kezdőlap Adatlap Ismerősök Bejövő üzenetek 1 Beállítások Kijelentkezés Keresés

**Fan Check** 

Üzenőfal Személyes adatok Értékelések Discussions

Tovább az alkalmazáshoz
Alkalmazás tiltása
StalkerCheck has been renamed FanCheck to comply with Facebook policies.
Információk
★★★★★ (1.8 / 5)
Eddig 5948 vélemény
Felhasználók:
havi aktív felhasználók száma: 6.443.120
Kategória
Összes
Ezt az alkalmazást nem a Facebook fejlesztette.
Rajongók

Fan Check Csak rajongók

**Fan Check** Love funny t-shirts? Become a fan now :).
<http://www.facebook.com/pages/Funny-T-Shirts/113591094099>
**Funny T-Shirts**
Termék: 5.323 rajongó
augusztus 9., 14:21 · Visszajelzések megtekintése (797) · Megosztás · Jelentem

**Fan Check** <http://demotivators.onoko.com/facebook.htm>
**Uniqueness**
Forrás: demotivators.onoko.com
You're one in a million. That means there are 6707 people, exactly like you.
augusztus 4., 16:46 · Visszajelzések megtekintése (1.215) · Megosztás · Jelentem

**Fan Check** :) **Facebook**
Forrás: demotivators.onoko.com
You're doing it wrong.

Hirdetés létrehozása
Nemzetközi Babahordozó Hét 
Babahordozás kezdőknek, haladóknak, kendősőknek, meitaosoknak, ergosoknak, babakocsisoknak, ölbevívősöknek és mindenki másnak.
Jelezd, hogy ott leszel-e!
Buy Montenegro Property 

fana.png

Érdemes megjegyezni, hogy nem létezik olyan alkalmazás, amely megmondja, mely ismerősünk írt/kommentelt a legtöbbet a dolgainkra.

Biztonsági kérdés

[módosítás](#)

Ezzel igazolhatod, hogy te vagy a fiók tulajdonosa.

Adatvédelem

[beállítás](#)

Állítsd be, milyen információkat szeretnél megosztani.

Fiókvédelem

[elrejt](#)

Hogy Facebook felhasználói fiókod a lehető legbiztonságosabb legyen, értesíteni tudunk, ha egy általad korábban nem használt számítógépről vagy mobil eszközről belépnek a fiókodba.

Szeretnéd, ha értesítenénk amennyiben új eszközről történik belépés?

☒ Igen ☐ Nem

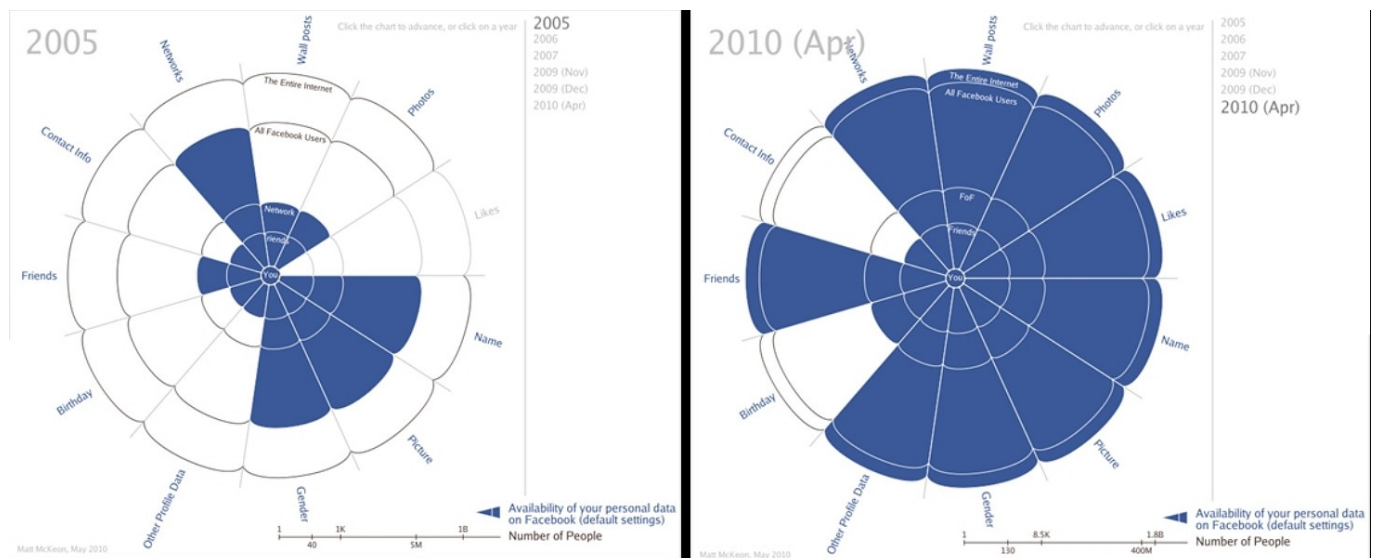
Küldés

Fiók felfüggesztése

[felfüggesztés](#)

fiokvedelem.png

Egy olyan hasznos biztonsági elem is található a Facebookon, amellyel a Gmailhez hasonlóan kézben tarthatjuk, milyen IP címről jelentkeztek be legutóbb fiókunkba. Akár e-mailes riasztást is kérhetünk az esetleges idegen belépésről.



mitoszt.png

Az évek során így változott a megosztott adatok aránya. Jól láthatóan egyre terebélyesedett a kör, amelynek középpontja a barátok, afölött a barátaink barátai, azt követi a minden Facebook tag, végül a külső kör pedig a teljes internet. Minden személyes dolgunkat nem igazán szeretnénk ennyire közkinccsé tenni.

facebook [Kezdőlap](#) [Adatlap](#) [Ismerősök keresése](#) [Profilom ▾](#)



This guy took a picture of his face Every day for 8 Years 

[Üzenőfal](#) [Adatok](#) [:D](#)

To see the Video - just click the button (No Survey). Enjoy :) 

[Ajánld ismerőseidnek](#)

57.228 ember kedveli ezt



[Conna Scrase](#) [Djavana Cameron Hammar](#) [Macaila](#)

Hivatkozások

3/374 hivatkozás [Összes megtekintése](#)

 [LikeFeed.BlogSpot.Com](#)
2010. augusztus 17. 18:39

 [7 Most Extreme Roller Coaster!!](#)
2010. augusztus 13. 18:12

 [10 World's Weirdest Stadiums](#)
2010. augusztus 11. 5:07

Oldal létrehozása saját cégem számára

Oldal jelentése



Facebook © 2010 · Magyar [Rólunk](#) · [Hirdetőknek](#) · [Fejlesztők](#) · [Álláslehetőség](#) · [Adatvédelem](#) · [Feltételek](#) · [Súgó](#)

video.png

Sose fogynak ki a csalók az érdekesnek látszó állítólagos videókból. Ha egy ilyen csak akkor lehet megnézni, ha előtte lájkolni vagy csatlakozni kell, inkább mondjunk le róla.

A Conficker féreg szótáralapú támadást indít a gyenge adminisztrátori jelszavak ellen. Így a fertőzés következményeinek kivédésében nagy szerep jut az erős jelszavak használatának

3: Change the root Password

Run "passwd" and type in your new password twice. Please note that your keypresses will not be displayed on the terminal screen (for security).

```
iPhone:~ root# passwd
Changing password for root.
New password:
Retype new password:
iPhone:~ root#
```

4: Change the mobile Password

This is the regular user account on the device. Run "passwd mobile" and repeat as directed above.

```
iPhone:~ root# passwd mobile
Changing password for mobile.
New password:
Retype new password:
iPhone:~ root#
```

cserelni.png

Csak azok a feltört telefonok vannak ilyen veszélyben, amiken fut az SSH-démon. Mivel a támadó programja nyilvánosságra került, ezért egy jailbreakelt iPhone telefontól is első dolgunk legyen az alapértelmezett jelszó megváltoztatása

http://www.phenoelit-us.org/dpl/dpl.html

Services Since: Oct 2007 Rank: 16779 Site Report [US] GoDaddy.com, Inc.

Default Password List

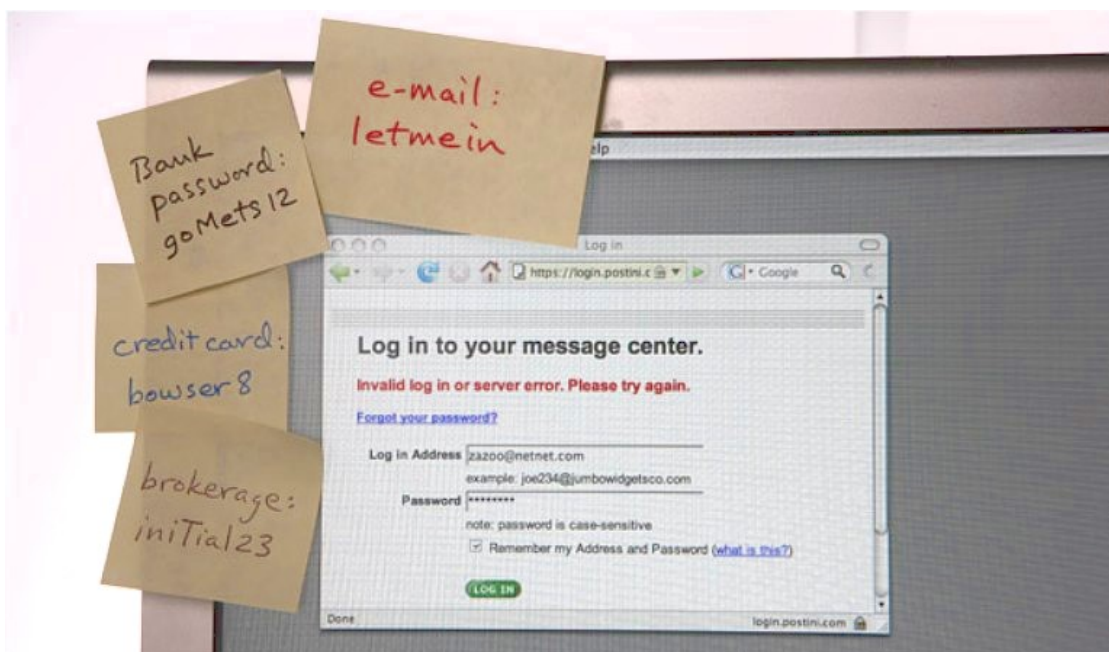
Last updated: 02.22.2010

Vendor	Model	Version	Access Type	Username	Password	Privileges	Notes
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	debug	synnet		
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	tech	tech		
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)		
3COM	LANplex	2500	Telnet	debug	synnet		
3COM	LANplex	2500	Telnet	tech	tech		
3COM	LinkSwitch	2000/2700	Telnet	tech	tech		
Huawei	E960			admin	admin	Admin	
3COM	NetBuilder		SNMP		ILMI	snmp-read	
3COM	Netbuilder		Multi	admin	(none)	Admin	
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD	Admin	
3COM	SuperStack II Switch	2200	Telnet	debug	synnet		
3COM	SuperStack II Switch	2700	Telnet	tech	tech		
3COM	OfficeConnect 812 ADSL		Multi	adminntd	adminntd	Admin	
3COM	Wireless AP	ANY	Multi	admin	comcomcom	Admin	Works on all 3com wireless
3COM	CellPlex	7000	Telnet	tech	tech	User	
3COM	cellplex	7000	Telnet	admin	admin	Admin	
3COM	cellplex	7000		operator	(none)	Admin	
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)	Admin	

Kész TMN: 'pakistan army tough root' Get video 68.178.254.188 // Tooltip// Icon

default.png

A Phenoelit az egyik legismertebb weboldal, ahol alapértelmezett jelszavakat találunk. A felhasználói lustaságra jellemző, hogy ezek alkalmazása többször jár sikerrel, mint kudarccal



eztne.png

Lehet bármilyen jó a jelszó, ha azt idegenek könnyen kifigyelhetik, vagy kis cédulákon magunk tesszük közkinccsé, úgy nem ér az egész semmit, megszűnik akadály lenni az illetéktelen behatolás útjában.

Check your password – is it strong?

Your online accounts, computer files, and personal information are more secure when you use strong passwords to help protect them.

Test the strength of your passwords: Type a password into the box.

Password:

Strength: **BEST**

Note: This does not guarantee the security of the password. This is for your personal reference only.

What is a strong password?

The strength of a password depends on the different types of characters that you use, the overall length of the password, and whether the password can be found in a dictionary. It should be at least 14 characters long.

Share this page: [M](#) [A](#) [D](#) [F](#) [T](#) [G](#) [S](#) [Y](#) [X](#) [B](#)

Security Tools, Scans, Updates

Download Microsoft Security Essentials (antivirus, antispyware)

Get a free PC safety scan for Windows Vista and Windows 7

Get a free PC safety scan for Windows XP

Help remove malware with the Microsoft Malicious Software Removal Tool

Get security updates from Microsoft Update

test.png

Több helyen is tesztelhetjük az új, tervezett jelszavunk erősségét. Ha egyaránt van benne kis- és nagybetű, szám és különleges karakter, valamint hosszabb, mint tíz karakter, akkor az már nem is rossz



Kézdőlap Családfa Ismerős Üzenet Utvonaltérvező Utcakereső Stat Felhasználó Sögu
Új hely hozzáadása Legszébb helyek Helyek listája Katalógus Földrajz Világú Időjárás



Ottlik Lilla Lea
• adatlapja

Legnagyobb családok
● (4467) Czaga Lászlóné
● (3668) Stiller Gábor cs
● (1278) Balogh Péter
● (942) Lőrincz Rozália c
● (841) Jotter családja
● (902) Tonka László cs
● (836) Kékési Nikolett c
● (666) Bogar's családja
● (635) Sipos Péter cs
● (622) Radayné Matyas
● (616) Marton Jánosné c
● (577) Harvay D
● (574) Bodi István cs
● (564) Orosz Gábor cs
● (544) Komiszár Tünde
● (505) Olvcs családja
● (503) Jutit Antal család
● (503) Balazs László cs
● (496) Fekete Andrea cs
● (496) Fekete László c

Készíts Te is családfát!

Legújabb hozzászólások

4 nap 18 óra
érkezett
Györfi Éva: Heló! Nagyon szépek a képek, nekünk legjobban a türkizkék tenger tetszett...
5 nap 3 óra
érkezett
bence: Üdv. Tünde! Szeretem ezt az országot nagyon!
5 nap 3 óra

Ottlik Lilla Lea adatlapja

Ottlik Lilla Lea a(z) "Koródi Leila családfája" elnevezésű, nyilvános családja résztvevője, melynek létrehozója: Koródi Leila.

Alapadatok

Vezetéknév: Ottlik
Utónév: Lilla Lea
Név, becenév: Ottlik Lilla Lea
Nem: nő

Személyes adatok

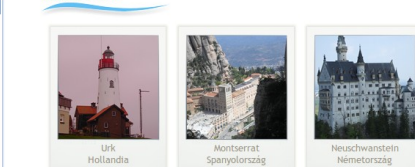
Születés ideje: 1972. május 28. vasárnap
Névnap: március 22.

Elérhetőségek

E-mail: leaottlik@magnaprodukcio.hu

Jelmagyarázat

nyilvános a nyilvános adatot bárki láthatja
védett a védett adatot csak az ismerősök és családtagjaid láthatják
zártkörű a zártkörű adatot csak a családfába felvett családtagjaid láthatják
titkos a titkos adatot csak te láthatod

Láttad már?

Címke felhő



Kézdőlap Családfa Ismerős Üzenet Utvonaltérvező Utcakereső Stat Felhasználó Sögu
Új Meghívó Kutatás Hozzájáruló Rajz Út Térkép Személy Naplár Fénykép Üzenőfal Stat Napló Tagok Beillesztés

**Családfa hozzájárulók**

A személyek felvitelét először a következő sorrendben olvassuk: először mindig a szülőket add meg, majd ha van, akkor a testvéreket, utána a kapcsolókat, és végül a gyomokokat!

1-21 követően mutass rá egy személyre. Az akkor megjelenő menüből válassz a "Hozzájárulók" menüpontot, annak érdekében, hogy az ő körüli hozzájárulóit is megadhasd.

1-22-vel a módszerrel felülíthod a teljes családfát.

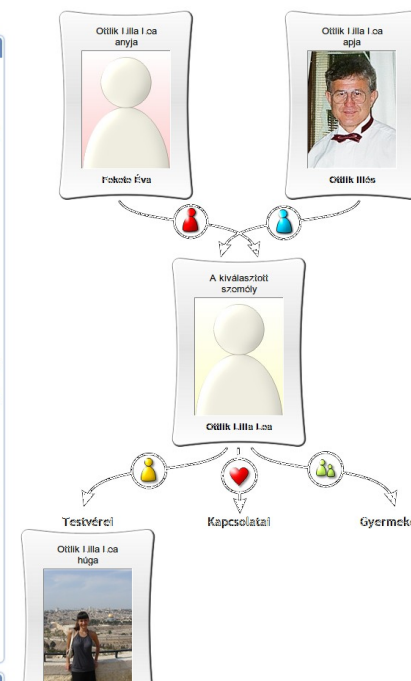
A hozzájárulók szorokozása pontos csak akkor nyílik lehetőséged, ha te vagy az adott családja közlője, vagy szorokozóval joggal felhívhatod tagja. Felhívás esetén csak megtekintheted az adatokat.

A hozzájárulók szorokozása egy egyszerű folyamat, sok sok lehetőséged. Ha még nem ismered azokat, akkor először, ha előbb a sugóban alaposan átnézel, majd az a feladatod, hogy a családod sora tartalmat majd hibákat, így sok későbbi bosszúságot, hibajavítástól kímélheted meg magadat!

Legnagyobb családok

Koródi Leila családfája Ottlik Lilla Lea hozzájárulói

Használati útmutató a sugóban: hozzájárulók szerkesztése.



Bejelentkezés
E-mail:
Jelszó:
☐ Automatikus bejelentkezés
[Regisztráció] [Jelszó?]
Bejelentkezés

Keresés
Google keresés:
itt voltam! webhelyen
☐ teljes interneten
☐ összetett kereső

**ottlik.png**

Komoly előny, ha valakit Kis Pálnak, vagy Kovács Józsefnek hívnak. A név gyakoriságból adódóan viszont egy Hagyó Miklósnak, vagy egy Ottlik Lilla Leának már nincs ekkora szerencséje, különösen ha előzőleg önként fel is töltöttek fel magukról, családjukról sőt teljes családfájukról egy rakat személyes információt nyilvános weboldalakra.



onetouch.png

Ha vásárolunk egy új kamerát vagy telefont, az úgynevezett extrák közt szerepelhet olyan funkció, amivel "egy kattintással" megoszthatunk képeket, videókat. Szerintünk ez nem hogy nem extra, hanem inkább hátrány: egy óvatlan vagy véletlen kattintással egy soha nem törölhető tartalmat is feltölthetünk.



kekosztriga.png

"Dolgozzál te hélóta, mert jönnek a spártaiak" Vegyük észre, az internet világában nincsen undo. Ha valaki meglegfelvonuláson vett részt, korábban pornósztráként kereste a betevőt, valamikor füvet szívott, vagy a múltban a Kék Osztriga Bár törzsvendége volt és erről képek is készültek, akkor azok szépen elő is fognak kerülni a megfelelő pillanatban: ha választások közelednek, és az illető parlamenti képviselő szeretne lenni, vagy éppen egy új állás sorsa forog kockán. Külön üzletág lett a lejárató információk megrendelése, bányászata.

<http://facebookmarketing.hu/2010/04/28/kozossegi-fejvadaszat/>



Have an account? [Sign in](#)



Get short, timely messages from Ozan İlbey Yılmaz.
Twitter is a rich source of instantly updated information. It's easy to stay updated on an incredibly wide variety of topics. [Join today](#) and [follow @ozanilbey](#).
[Let me in >](#)
Get updates via SMS by texting **follow ozanilbey** to your local code.
[Codes for other countries](#)



ozanilbey

Açıköğretim ayağına açık açık geçiriyorlar. Böyle sınav mı olur be!
8:38 AM May 29th via web

Geber alerji, geber!
9:10 AM May 23rd via web

...and engineers are now officially banned from all future philosophy conferences: <http://bit.ly/9x6fys>
5:11 AM May 22nd via web

Zararın hiçbir yerinden dönemiyorsan kar edemeyeceksin demektir.
7:35 AM May 20th via web

Tweet Number 300: This is SPARTAAAA!
12:33 PM May 19th via web

Güzel fakültemin güzel insanları: <http://bit.ly/ckBooc> #metuarch
12:30 PM May 19th via web

Official Twitter App for iPhone: <http://bit.ly/bu4gSu>
12:19 PM May 19th via web

Artık ODTÜ Mimarlık Fakültesi ile ilgili Twitter iletilerini tek kanalda toplamak şart oldu. Hepsinin sonuna #metuarch.
2:50 AM May 19th via web

iCade - iPad Arcade Cabinet: <http://bit.ly/dzmF3r>
12:25 AM May 19th via web

Name Ozan İlbey Yılmaz
Location Ankara / Turkey
Web <http://www.ozanilbey.net>
Bio I am experienced in Graphic Design and Web User Interface Design. I have a big passion and a bit obsession for these fields.
117 following 127 followers 8 listed

Tweets 304

Favorites

Lists
[@ozanilbey/it-specialists](#)
[@ozanilbey/services](#)
[@ozanilbey/firms](#)
[@ozanilbey/friends](#)
[@ozanilbey/artists](#)
[@ozanilbey/design](#)
[View all](#)

Following

[View all...](#)

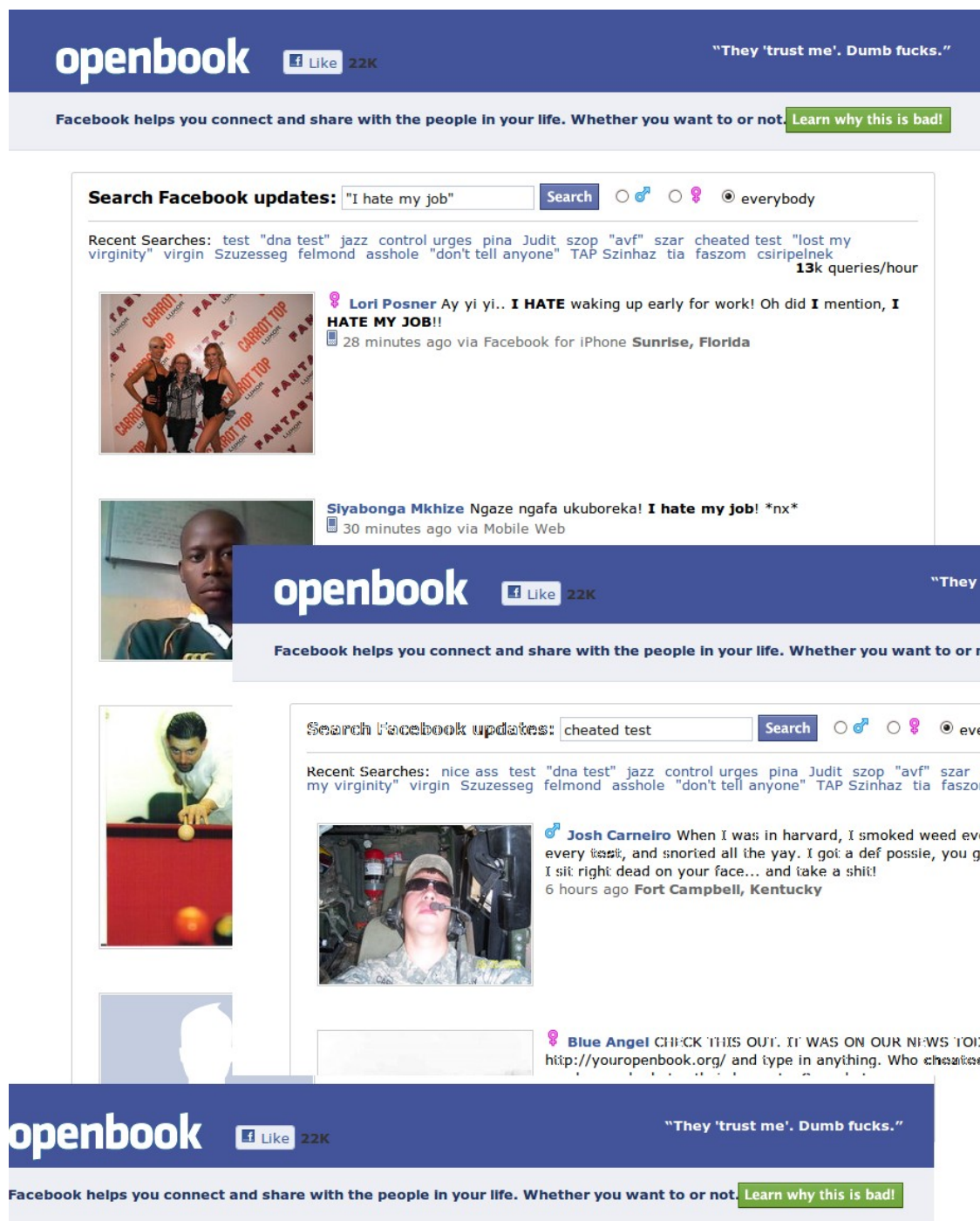
yilmaz.png

Hibátlan program nem létezik, csak olyan, amely eddig esetleg hibamentesen futott le. Egy élelmes török internetező, Ozan Yılmaz vette észre, hogy egy egyszerű script kód segítségével bárkit a Twitter követői közé tud varázsolni. Egy másik esetben a Facebook értesítő levelekből kinyerhető volt az eredeti feladó IP címe. Ezeket a hibákat azóta állítólag már kijavították. Vajon hány lehet még?



airport.png

Egy 26 éves brit férfi azt a viccesnek gondolt üzenetet küldte ki a Twitteren, hogy felrobbantja a repteret, ha késik a gépe. A rendőrség azonban nem tartotta ezt viccesnek, emiatt Paul Chamberst letartóztatták, végül aztán megúszta annyival, hogy pénzbüntetést kellett fizetnie.



openbook.png

Az Openbook egy szemléletes jó példája, mennyire könnyű terhelő adatot gyűjteni. A publikus megjegyzésekből - és lassan már csak ilyen van - olyan kínosakat gyűjt ki, mint például ki mondott olyat, hogy utálja a főnökét, elvesztette a szüzességét, tett-e rasszista megjegyzést vagy ismerte be egy gyenge pillanatában, hogy csalt a vizsgákon.



Facebook Adatvédelmi Útmutató

Szerkeszd információid megoszthatóságát könnyen és egyszerűen.

Adatvédelem a Facebookon

Az adatvédelem a következőkön alapul: Rendelkezz te az általad megosztott tartalmak felett. Legyen egyszerű a barátaiddal való kapcsolatfelvétel. Az adatvédelmi beállításaid pedig legyenek egyszerűek és könnyen megérthetőek.

Friends

Friends of Friends

Everyone

A Facebook-on három alapvető biztonsági szint létezik: **Barátok**, **Ismerőseim**, **Ismerőseim**, **Mindenki**. Ezeken kívül létezik egy csomó nyilvános információ, amely segít a barátaidnak, hogy megtaláljanak, és kapcsolatba lépjenek veled: a Neved, Profilképed, Nemed, és a meglévő Kapcsolataid. Ebben benne vannak az ismerőseid, hálózataid, és az Oldalak, amelyekhez csatlakoztál. Azt is mindig szabályozhatod, hogy



Adatvédelmi újdonságok

Nézd meg, hogy az aktuális változások hogyan hatnak az adatvédelemre és hogyan tudod szabályozni ezeket.

"Tetszik" és Facebookon kívüli kapcsolódás más módok

Olvass a változásokról

Nézd meg, hogy működik

Keress választ a gyakori kérdésekre

Szerkezd a **Azonnali** személyreszabás, Bejegyzéseim és Amiket szeretek adatvédelmi beállításait

adatved_utmutato.png

Nem egyértelmű, ki tehet jobban a jelenlegi káoszról: a felhasználók, akik nem olvassák el az adatvédelmi irányelveket, vagy az ezt vastagon kihasználó, és a szétkürtölést alapértelmezettnek beállító üzemeltetők. Az adatkezelési szabályzatának egyik pontja szerint az abban foglaltakat bármikor egyoldalúan módosíthatják - de nincs ez másként a magyar Iwiw esetében sem. Lehetne persze minden alaphelyzetben biztonságos állapotban, de akkor a "felhasználói élményre" hivatkozva nem tudnának tömeges forgalmat generálni. A forgalmi, viselkedési, kapcsolati adat pedig érték, a reklámozni kívánó cégek pénzt fizetnek érte az üzemeltetőknek.

Privacy Check

Your privacy score is 18/21 [What does this mean?](#)
Happy with your score ? Then [share it with your friends](#) and see what score they get.

profile data [view raw data](#)

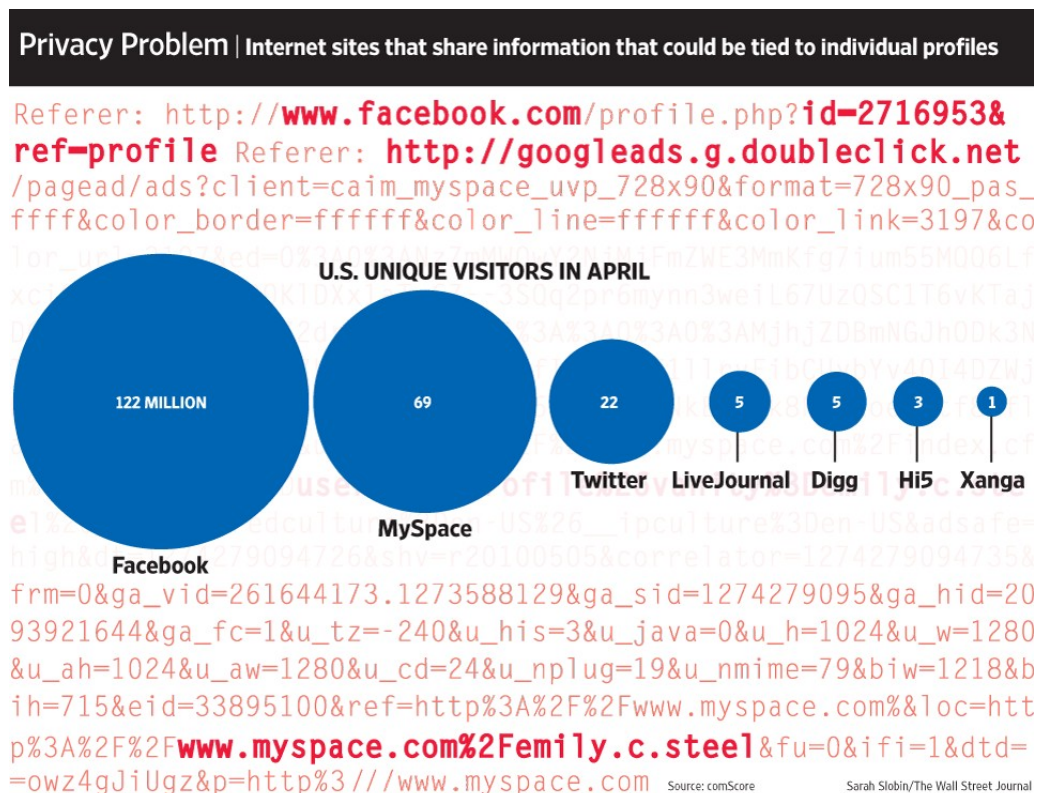
Facebook ID: [REDACTED]	Name: Istvan [REDACTED]
Birthday: -	Gender: -
Relationship status: -	Timezone: 2
Hometown: -	Location: -
School(s): -	Employer(s): -

other data

Facebook
Like
Donate
Here are some
• [Facebook](#)
• [The Edge](#)
• [7th](#)

pcheck.png

Jó néhány alkalmazás jelent meg, amelyekkel ellenőrizni lehet az adatvédelmi beállításokat, például Reclaim Privacy, vagy a Facebook Privacy Check.



problem.png

Nem Mózes örökérvényű kőtábláit nézzük, az biztos. Szinte havonta változik a felhasználói szerződés, és egyre tágabb teret enged az információk áramlásának. A Facebook ezt "fejlődésnek" hívja, az Electronic Frontier Foundation inkább rombolást emleget.

f My friends who like The Ellie Fund and live in Boston, Massachusetts



Allan Saunders
carpenter and cabinet maker at Carpentry Masters
👤 Your friend since May 2008
🏠 Lives in Boston, Massachusetts
👍 Likes The Ellie Fund, Human Rights Campaign and 2 others
👥 93 mutual friends including Peter Asklund and Diane Griffin

★ Friends Message 🔍



Julie Lerner Nations
Executive Director at The Ellie Fund
👤 Your friend since May 2012
🏠 Lives in Boston, Massachusetts · From Buffalo, New York
👍 Likes The Ellie Fund, Social Media for Nonprofits and 74 others
👥 6 mutual friends including Joe Waters and Kurt Steiner

✓ Friends Message 🔍



Tara White Griffith
Board Member at The Ellie Fund

👤
🏠
👍
👥
✓

Facebook's Graph Search lets people discover shared interests and connections.

facebook-privacy.png

Lehet persze csak névvel és egy darab fotóval is fent lenni, és közben okosnak gondolni magunkat. Nem árt tudni azonban, hogy amikor a Facebook eladhatja az adatainkat, akkor annak csak egy kisebb része az esetleg nem kitöltött személyes adat. Ennél is érdekesebb és értékeesebb lehet a kapcsolati háló, az üzeneteink, és rendszerbeli viselkedésünk, eddigi kattintásaink története.

General

Security

Privacy

Timeline and Tagging

Blocking

Language

Notifications

Mobile

Followers

Apps

Ads

Payments

Support Inbox

Videos

Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	Public	Edit
Review all your posts and things you're tagged in			Use Activity Log
Limit The Audience for Old Posts on Your Timeline Close			
! If you use this tool, content on your timeline you've shared with friends of friends or Public will change to Friends. Remember: people who are tagged and their friends may see those posts as well. You also have the option to individually change the audience of your posts. Just go to the post you want to change and choose a different audience. Learn about changing old posts Limit Old Posts			
Who can contact me?	Who can send you friend requests?	Everyone	Edit
Who can look me up?	Who can look you up using the email address you provided?	Everyone	Edit
	Who can look you up using the phone number you provided?	Everyone	Edit
	Do you want search engines outside of Facebook to link to your profile?	Yes	Edit

[About](#)
[Create Ad](#)
[Create Page](#)
[Developers](#)
[Careers](#)
[Privacy](#)
[Cookies](#)
[Ad Choices](#)
[Terms](#)
[Help](#)

settings.png

Huszonvalahány különböző adatvédelmi beállítás. Van akit ez elriaszt attól, hogy egyáltalán állítgasson bármit is. És az alapértelmezett állapot rendre "igen, az egész Univerzummal meg akarom osztani" opció. A sűrű cikkezés hatására talán végre elindult egyfajta öntudatra ébredés.

tenyleg ott figyel.... :O

(6 hours ago)

just found some Treasured Golden Mystery Eggs and wants to say thank you!

(6 hours ago)

has completed a collection in FarmVille!

(6 hours ago)

is working hard on a Botanical Garden in FarmVille!

farmville.png

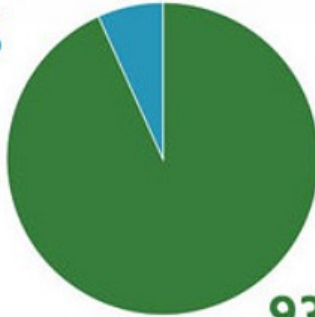
Minden egyes alkalommal, ha például a 83 millió virtuális farmer valamelyike a FarmVille mezőgazdasági szimulációs játékkal, vagy a MaffiaWars-szal játszik, megengedi, hogy letöltsék a profilját és továbbadják az adatait egy harmadik félnek. Az ismeretlen harmadik féllel pedig semmilyen szerződéses viszonyban nem vagyunk.

Sharing info with others.

Would you have liked Facebook to have required you to "opt-in" to sharing rather than "opt-out"?

No, I don't mind having to "opt-out"

6.78%



93.22%

Yes, I would have preferred to "opt-in"

Source: Sophos poll, 605 respondents
26-27 May 2010

optin.png

A józan ész, de a Sophos miniszavazás szerint is a "zárt, és majd mi engedélyezzük, ha akarjuk" modell lenne a kívánatos. Természetesen a Facebook üzemeltetők pont ennek az ellenkezőjét gondolják jónak és alapértelmezettnek.



oktatas.jpg

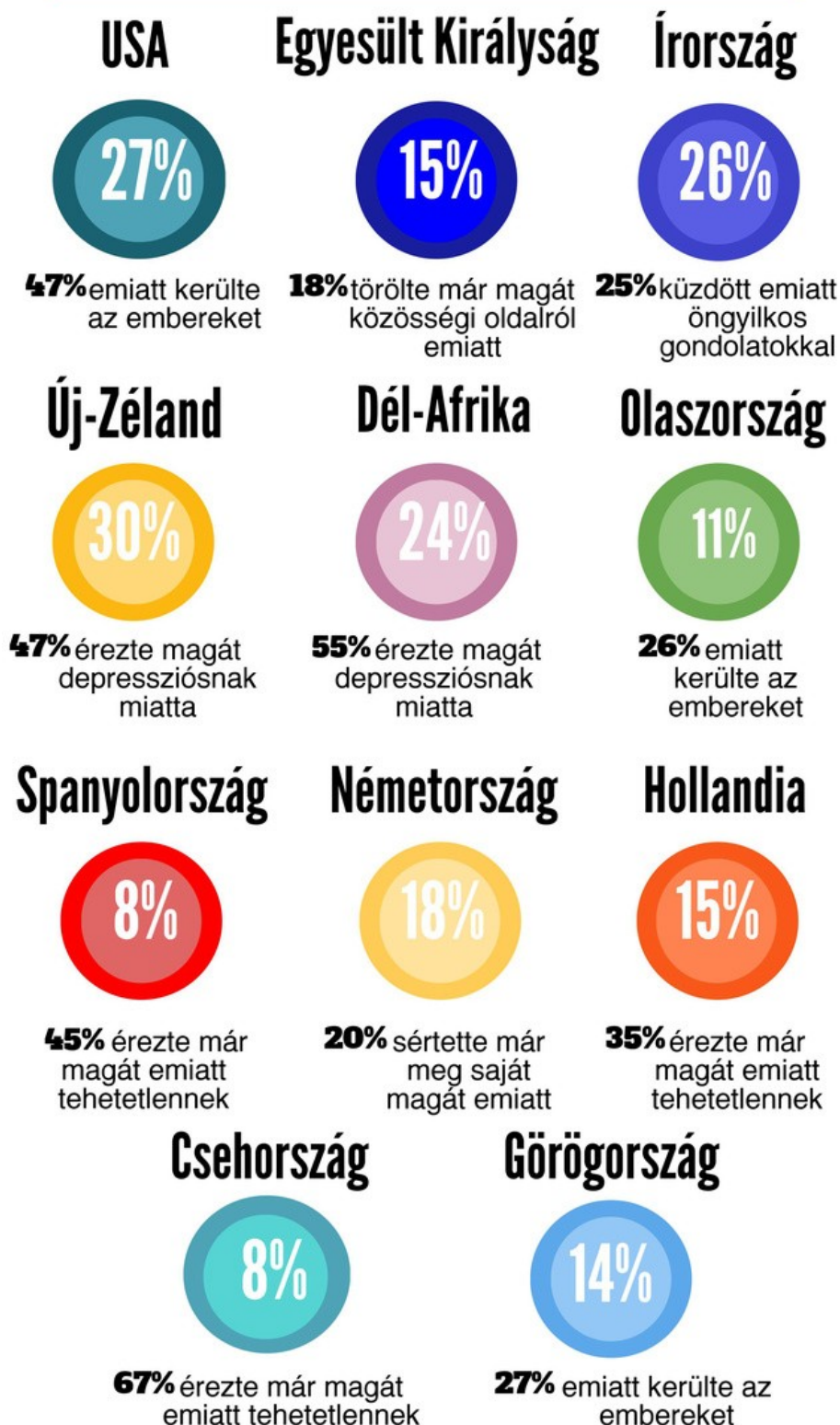
Az oktatás is teljesen átalakult, még az általános iskolában tilthatják vagy beszédhetik reggelente, de a középiskolában és a felsőoktatásban a diákok folyamatosan csetelnek, sokszor real time ellenőrzik is a tanár mondandóját az interneten



muzeum.jpg

A valóság helyett a kütyükbe való belefeledkezés, minden szabad perc „kihasználása” eléggé jellemző tünet a mai gyerekekre.

Az internetes zaklatást elszenvedett kamaszok aránya, százalékban*



*A Vodafone felkérésére a YouGov által 11 országban, 4 720 kamasz megkérdezésével elvégzett felmérés. A fent ismertetett kérdésben arról érdeklődtek a kamaszoknál, hogy estek-e már internetes zaklatás áldozatául.

zaklatas.jpg

A Vodafone nemzetközi felmérése az internetes bántalmazásról, zaklatásról. A kamaszkorúaknak komoly problémákat okoz a jelenség világszerte.



metro.jpg

Ha majd mindenkinek a fején virtuális sisak lesz, akkor vajon ki fogja átadni az ülőhelyet a kismamáknak és az öregeknek?

FIGYELSZ RÁJUK?

A gyerekbántalmazás formái

ELHANYAGOLÁS

gyerek nem kap enni | nem kap gyógyszert,
ha beteg | nincs megfelelő ruhája | nem
tisztálkodhat | nincs megfelelő fekhelye |
nem járhat iskolába/óvodába | fázik | nem
foglalkoznak vele



FIZIKAI ERŐSZAK

pofozás | verés | rúgás | megkötözés |
bezárás | hajhúzás | égetés | rázás |
megszúrás



SZEXUÁLIS BÁNTALMAZÁS

intim testrészek mutatása a gyerekeknek | szexuális kapcsolat
létesítése | szexuális tartalmú sztorik, viccek mesélése a
gyerekeknek | a gyerek bevonása telefonon vagy interneten
közvetített szexuális tartalmakba | pornográf képek, filmek
mutatása a gyerekeknek

ÉRZELMI BÁNTALMAZÁS

kirekesztés | a teljes közöny | keresztülnézés
megalázások | csúfolás | viccek álcázott bántás
| fenyegetés | állandó kritizálás



unicef.hu/hogylehet



unicef.hu@unicef-jogsegely

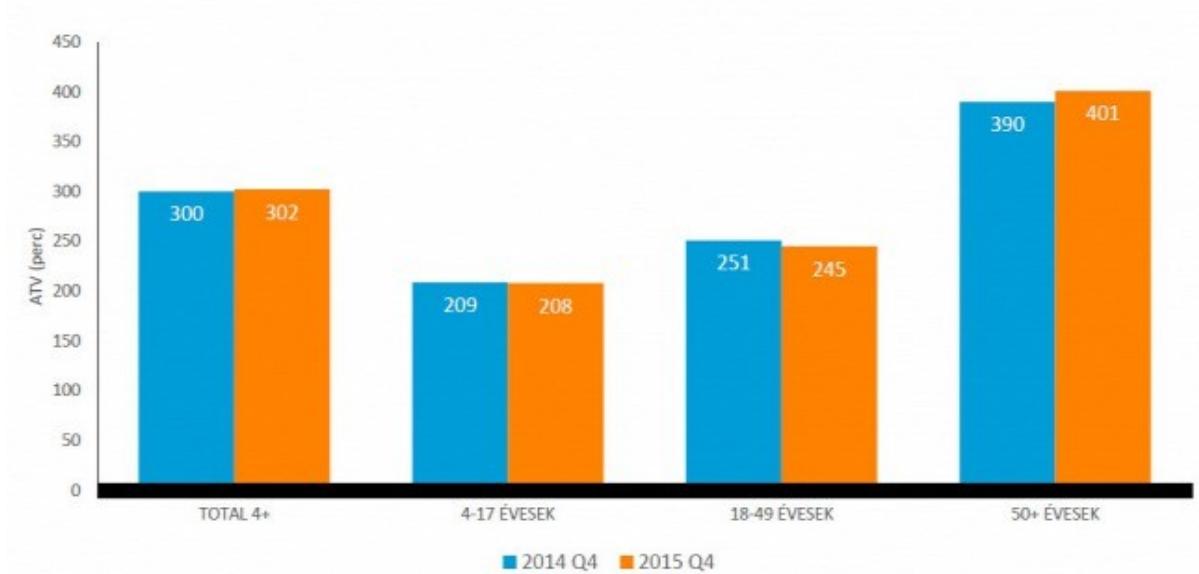
unicef
MAGYAR BIZOTTSÁG

gyermekbantalmazas-unicef.jpg

A gyerekbántalmazás jelei, amire a környezetnek fontos figyelnie.

EGY FŐRE JUTÓ NAPI TÉVÉNÉZÉSI IDŐ

2014. és 2015. IV. negyedév, Live+Playback



tvnezes.jpg

A napi televíziónézés statisztikái. A 4-17 évesek is 200 perc felett járnak naponta.



A sok egymásnak ellentmondó cikk után végre itt a bizonyíték, a népszerű színész tényleg jobban van. Nagy szakállt növesztett, botra támaszkodik, de tud már egyedül menni, és társalogni is képes. Gyógyul meg, János!

2016.05.10. 03:00 | kbv

[Ajánlom](#) [Megosztás](#) [3](#) [Kommentál](#) [Kérlek](#)

Botjára támaszkodva szakállas férfi sétál görnyedten az idegtudományi intézet parkos kertjében egy hölgy kíséretében – sok szemlélőnek valószínűleg csak ennyi tűnt fel hétfő délelőtt az Amerikai úti kórházban. Pedig a szakállas férfi Kulka János volt, a korábban életerős színész, aki jellegzetes hangjával és sármájával egy országot varázsol el estéről estére. De aggodalomra így sincs ok, annak ellenére, hogy Kulka elsőre tragikusan fest a tőle szokatlan rendezetlen ábrázattal – sapkában és melegítőben –, valójában óriási siker és a gyógyulás felé vezető út biztos jele az, hogy egyáltalán feltűnik az udvaron. Nővére, Janina kísérte le kicsit napozni és beszélgetni.



Sapkában, szakállal, Kulka a nővérel beszélgetett © Bors

Az alaposan lefogyott színészt a Bors olvasóriportere fotózta le – jár neki a 15 ezer forint –, s elmondta: látta, hogy **a művész képes egyedül járni, és rövidebb sétákat is megtenni**, igaz, négy lábú botja nélkül még bizonytalan a mozgása. A testvérek hosszadalmas beszélgetéséből pedig úgy tűnt, Kulkának már a szavak megformálása sem esik nehezére, folyékonyan társalog, élénken gesztikulál. János és Janina egy napsütötte széket választott az ejtőzésre és a tavaszi napsugarak kiélvezésére, és talán az a legjobb jel, hogy amikor Kulkának melege lett, maga vette le kapucnis pulcsiját. Ebből ugyanis arra lehet következtetni, hogy **a négy héttel ezelőtti stroke-ját követően jobb karja is kezd visszanyerni az összes funkcióját**. Egyvalami pedig egyáltalán nem változott a színészen: még ebben az állapotban is képes mosolyogni.



A színész képes rövidebb utakat is megtenni, igaz, négy lábú botja nélkül még bizonytalan a járása © Bors

LEGFRISSEBB

- 10:00 Pálmamagköt cumiztatja a borzokat Henrietta
- 09:36 Késes támadás egy megállóban: meghalt az egyik áldozat
- 09:30 Nem tudná pénzé tehetségét az Alpok Adria királynője
- 09:00 Ádám keresi Évát: szörnyű tragédia emlékeivel el Klóé
- 08:30 Nem csak Biskut temették el titokban

MÉG TÖBB CIKK!

Partnereinktől

hirdetés

LEGNÉPSZERŰBB



Sérülés miatt hagyják ki az Eb-t



Palvin Barbara: a pénz nem boldogít - a hét aranyképesei



Tizen, vascsúvekkel ültetették - áldozataikat Zsolték



Helyreigazítás



Ezzel a trükkel tuti kiderül, ha valakinek műmelle van - videó

MÉG TÖBB CIKK!



AIÁNDÉKOZZON

bors_15ezer.jpg

Az átlagos erkölcsi szintet nem csak az mutatja jól, mennyien olvasnak irodalom helyett bulvár újságokat, de itt az is bevett szokás, hogy a hírességeket intim helyzetekben titokban lefotózó úgynevezett „olvasóriporter” ezekért pénzt kap a szerkesztőségtől. Itt a súlyos beteg Kulka Jánost fényképezte le valaki a kórházban 15 ezer forint jutalomért - az adatvédelmi elvekre fittyet hányva.

A 16 éves Jessica Laney-t **otthonában találták holtan**, miután rendszeresen lekurválták és öngyilkosságra bízatták. A zaklatásról nem tudott sem a családja, sem a barátnője.

Írorszában a 15 éves Ciara Pugsley lett öngyilkos a házukhoz közeli erdőben, miután ask.fm-en csúnyának és kurvának nevezték.

Hat héttel később, szintén Írorszában a 13 éves Erin Gallagher **lett öngyilkos** az otthonában. 24 órával a halála előtt válaszolt egy feltett kérdésre, amelyben fizikai erőszakkal fenyegették meg. „Szerinted vicces, ahogy piszkálsz engem ask.fm-en? Ja, valószínűleg vicces volt, és viccesnek fogjátok gondolni, amikor kötelet kötök a nyakamra?” Pár héttel később a nővére Shannon is véget vetett az életének.

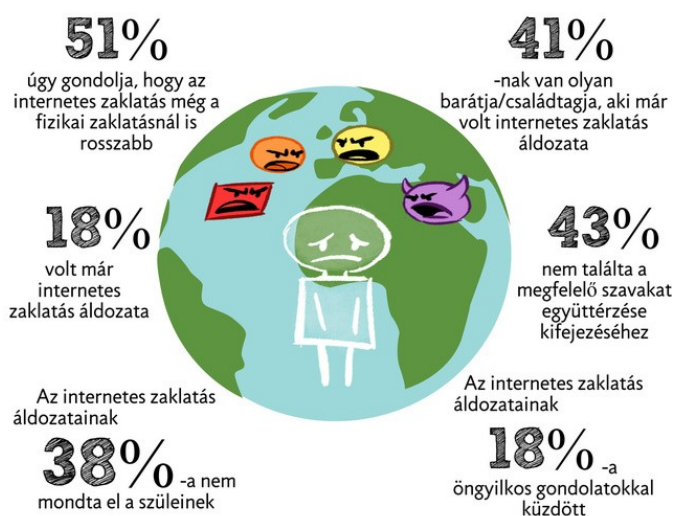
Angliában, Leicestershire-ben, egy 14 éves lány, Hannah Smith lett öngyilkos, miután az oldalon **azt mondták neki**, hogy haljon meg. A család az oldal azonnali betiltását követeli, petíciójuk 45 ezer támogatónál tart.

Ez volt az az eset, ami után David Cameron brit miniszterelnök **sem maradt csendben**.

brit.jpg

Sajnos az is előfordul, hogy a súlyosan és folyamatosan zaklatott fiatalok közül néhányan az öngyilkosságra menekülnek.

A kamaszok 43%-a a kábítószerrel való visszaélésnél is nagyobb problémának tartja az internetes zaklatást*



*A Vodafone felkérésére a YouGov által 11 országban, 4 720 kamasz megkérdezésével elvégzett felmérés

bul1.jpg

A kamaszok 43%a a kábítószerrel is komolyabb problémának tartja az internetes zaklatást.

COUB Search Featured Popular Sign up Log in Create



Király Linda és a Himnusz (Banned video: Hungarian bimbo star tries to sing the national anthem)
LSD Channel Hungary · Mar 11, 2014 · 4,964 views · from Youtube

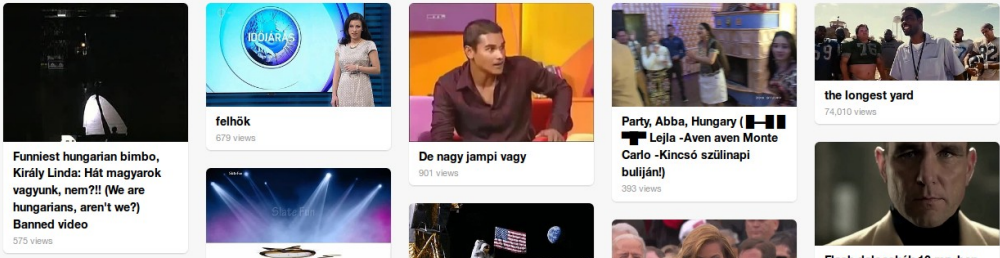
Facebook Tweet Reddit ... Embed

LSD Channel Hungary
surreal
2,390 coubs · 1,766 recoubs

Original video
Király Linda és a Himnusz
Coub It!

#kiraly linda #hymn #baki #funny
#bimbo #vices #enekel ...

More from LSD Channel Hungary



Suggested

Funniest hungarian bimbo, Kiraly Linda: Hat magyarok vagyunk, nem?! (We are hungarians, aren't we?) Banned video
575 views

felhök
679 views

De nagy jampi vagy
901 views

Party, Abba, Hungary (Lejla -Aven aven Monte Carlo -Kincsó szülinapi buliján!)
383 views

the longest yard
74,010 views

Flash halmekek 10 m...ben

kiralylinda.png

Az internet nem felejt - ez egy komoly tanulság mindenki számára. Király Linda kínos esetét a Himnusz elfelejtett szövegével még tíz év után is őrzik az olyan megosztók, ahova a letiltás eszközei nem érte el.



cybersecurityinfographic.jpg

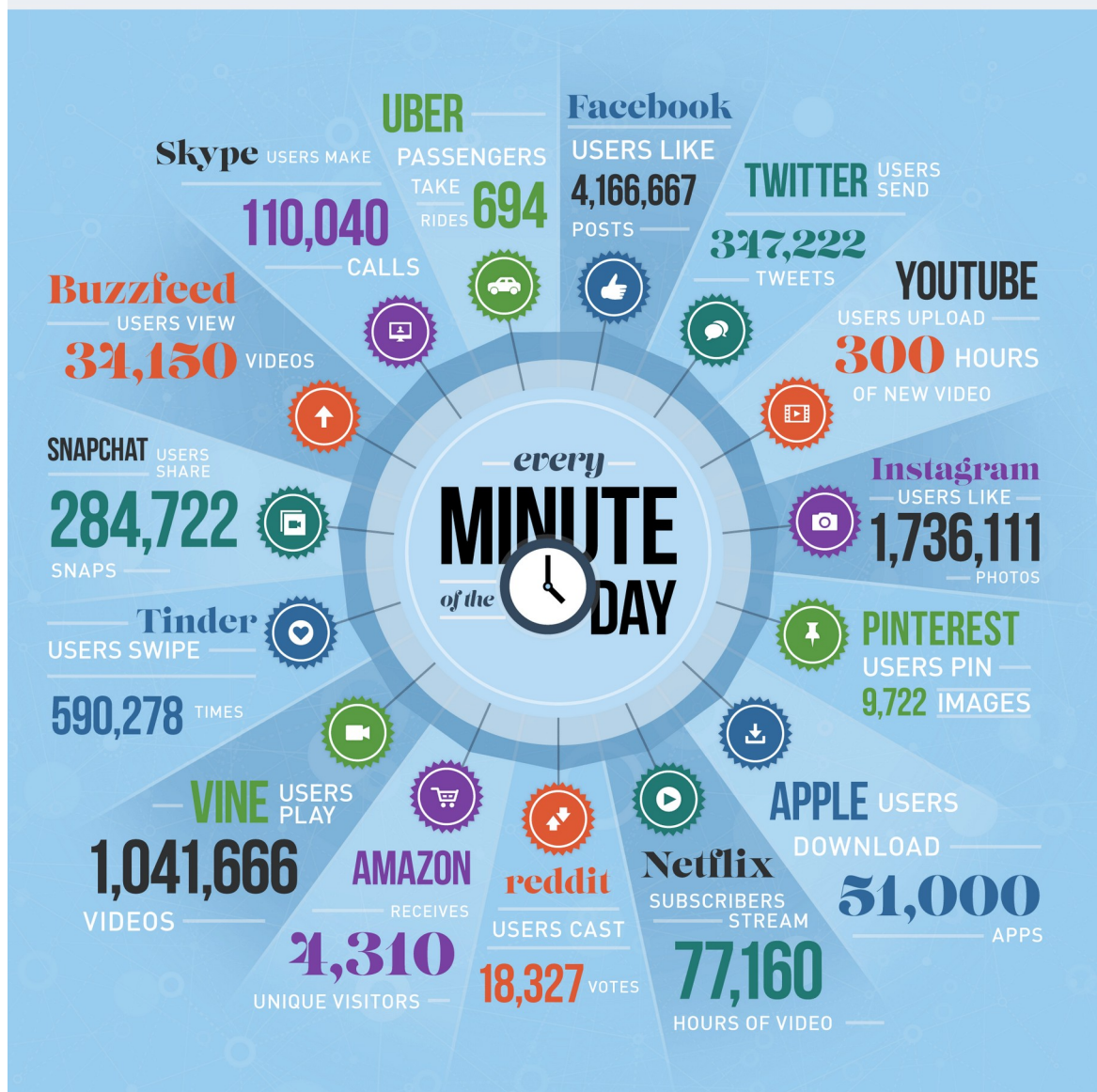
A felmérés szerint már a 2 éves kor alattiak 38%-a használ valamilyen mobileszközt, és 11% azoknak a tinédzsereknek az aránya, akik ki tudják kapcsolni a szülői felügyelet alkalmazást.



DATA NEVER SLEEPS 3.0

How much data is generated **every minute?**

Data is being created all the time without us even noticing it. Much of what we do every day now happens in the digital realm, leaving an ever-increasing digital trail that can be measured and analyzed. Just how much data do our tweets, likes and photo uploads really generate? For the third time, Domo has the answer—and the numbers are staggering.



THE GLOBAL INTERNET POPULATION GREW 18.5% FROM 2013-2015 AND NOW REPRESENTS

3.2 BILLION PEOPLE.

With each click, share and like, the world's data pool is expanding faster than we can comprehend. Businesses today are paying attention to scores of data sources to make crucial decisions about the future. The team at Domo can help your business make sense of this endless stream of data by providing executives with all their critical information in one intuitive platform. Domo delivers the insights you need to transform the way you run your business. [Learn more at www.domo.com](http://www.domo.com).



SOURCES:

FACEBOOK, TWITTER, YOUTUBE, INSTAGRAM, PINTEREST, APPLE, NETFLIX, REDDIT, AMAZON, TINDER, BUZZFEED, STATISTA, INTERNET LIVE STATS, STATISTICBRAIN.COM

data_never_30.png

Mi történik az interneten 1 perc azaz 60 másodperc leforgása alatt? 4 millió Facebook lájk, és 347 ezer új Twitter bejegyzés keletkezik, és többek közt 1.7 millió képet töltenek fel az Instagram oldalaira világszerte.



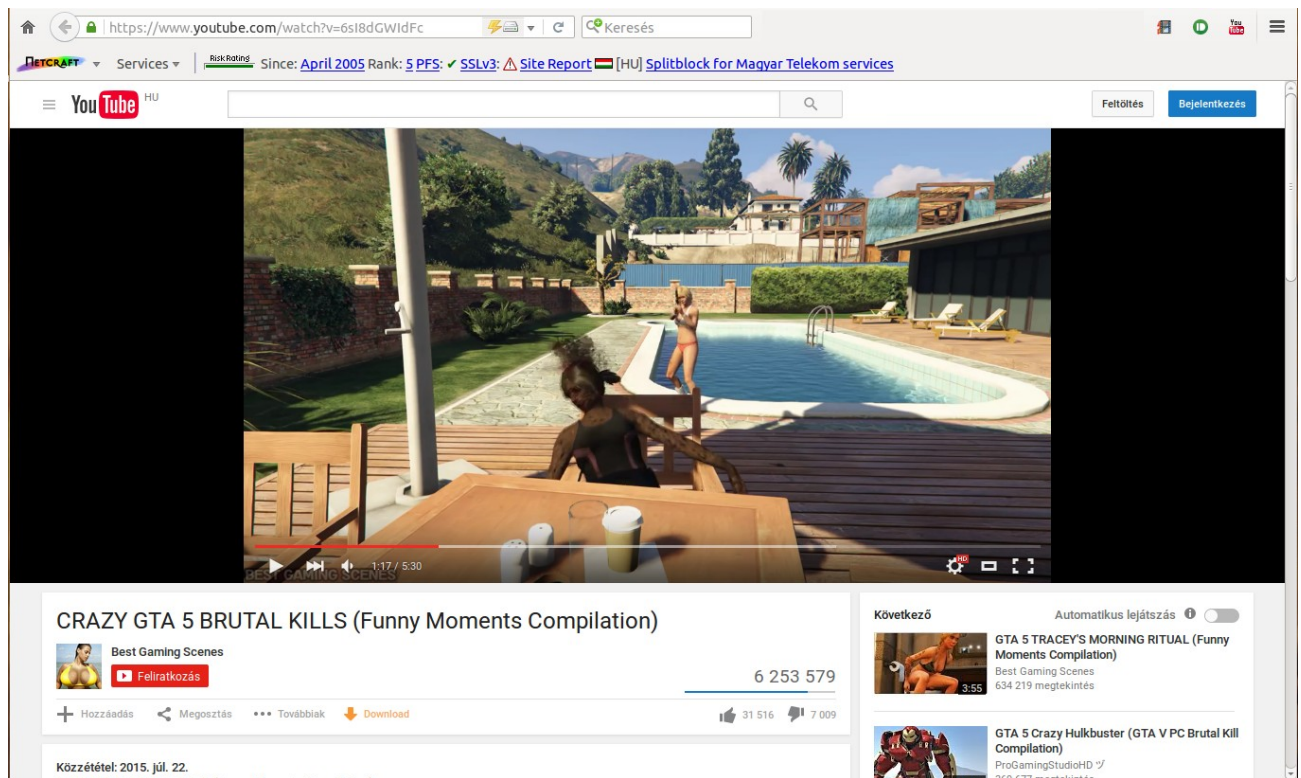
evilwithin.png

A számítógépes játékok többsége már valamilyen verekedős, lövöldözős, zombis vonalat követ. Az Evil with in azonban még ezek közt is a félelmetesebbek közül való, a dobozán nem véletlenül szerepel a 18-as karika.



gamerdeath.jpg

2015. januárjában egy 32 éves tajvani férfi meghalt, miután 3 napon keresztül folyamatosan játszott a számítógép előtt. A munkanélküli férfi egy internetkávézóban ült le a gép elé, és annyira belefelejtkezett a napokig éjjel-nappal tartó online szerencsejátékba, hogy három nap múlva belehalt.



gta_brutal.png

A GTA V, azaz Grand Theft Auto 5 nagy népszerűségnek örvend. Az autós, üldözős virtuális valóságban szinte mindent megtalálunk: vezethetünk repülőt, motorcsónakot, autókat. Azonban a 18 karikás játékban sztriptíz bárók, agyvelőfröccsenéssel járó kivégzések, agyonverés, mások szerelmi együttlétének kukkolása, és még sok minden hasonló - nem kiskorúaknak szánt - elem is szerepelnek, sokszor egy küldetés részeként.

Games

The Upcoming Zombie Games of 2015 & Beyond

Published 12:17 pm EST, January 9, 2015 | Updated 5:51 pm EST, July 9, 2015 | 5 Comments | By Bobby Bernstein 🔥 42.3k



Share



Tweet



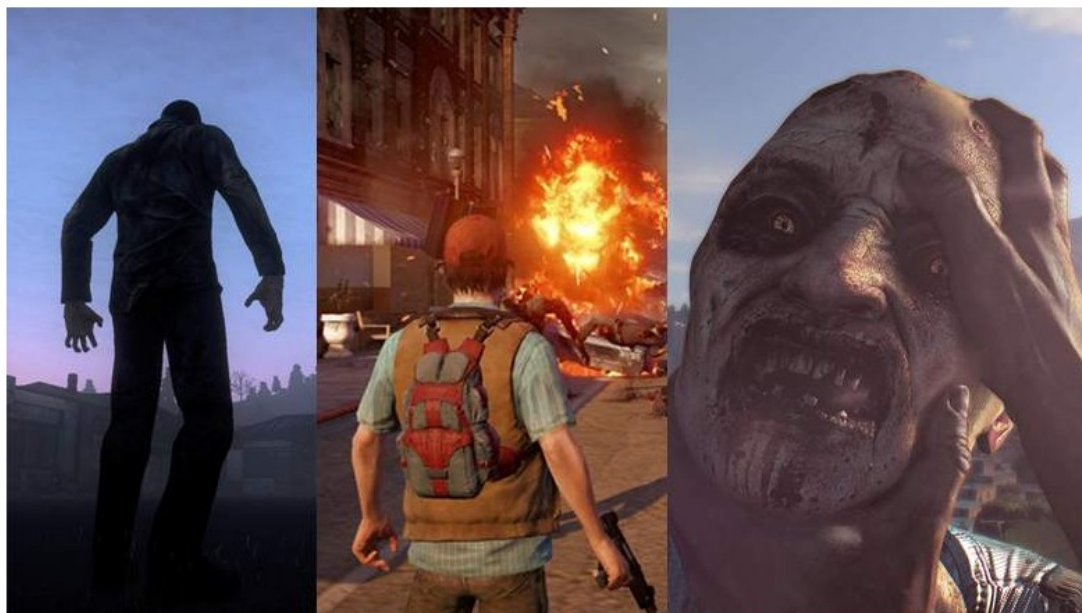
Share



Email



Follow



Top 5 Best Gaming Laptops Under \$1,000 2015

Looking to buy a cheap gaming laptop? Here are the 5 best gaming laptops for under \$1,000.

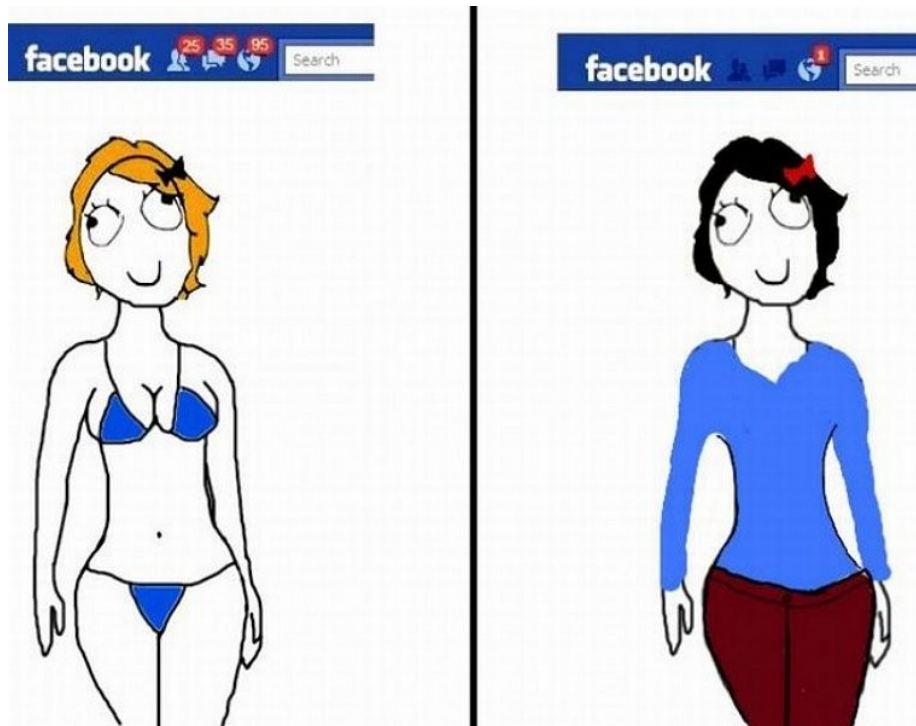
[Click here to read more](#)

****Update 4/30: *Dead Island 2* has been delayed into 2016, with Deep Silver noting that the game simply wasn't as ambitious as their initial vision. Bummer.****

Zombie games are a staple in the wonderful world of video games, and 2015's release schedule shows that zombie games are still as popular as ever. We've got 6 upcoming zombie games in queue for 2015, and some of them look truly great. And even the ones that don't look "great" will still be good, because, well, they're still zombie games. Games starring our undead friends have come a long way since the 90s, when games like *Zombie Nation*, *Zombies Ate My Neighbors* and *Corpse Killer* invaded our living rooms — during the heyday of zombie culture. And hopefully, we'll see more zombie games revealed at [E3 2015](#). So if you're into killing zeds, zombies, walkers, undeads, biters, the risen, the living dead, or z's, and want to do so this year, we've got you covered.

heavy_com.png

Érdemes néha utánanézni, mivel játszik a gyerek. Cikk a 2015-ös év slágerjátékairól.



tartalom.jpg

A mellékelt rajz jól rávilágít arra, hogy nők fürdőruhás képei bármikor bármilyen más tartalomról képesek elvonni az internetezők figyelmét.

A hatékony védekezés 3 alappillére:

1. Biztonsági alkalmazások használata

- A biztonsági termékek kiválasztása nem szimpla ár kérdés
- Technikai megbízhatóságon és bizalmon kell, hogy alapuljon
- A csak cloud védelem nem elegendő (pl. nincs védelem, ha nincs internet kapcsolat, vagy ha kompromittálják a központi menedzsment részt)

2. Hibajavítás, frissen tartás

- Automatizált patchmanagement
- Nem csak OS, hanem minden alkalmazás, virtuális környezet is

3. Biztonságtudatosság, képzések

- Folyamatos és rendszeres
- Hatalmas terület ez, pl. titkosítás, mentés, stb.
- Nem csak technikai, hanem social engineering is



3pillar.jpg

A számítógépes biztonság három alap pillére: biztonsági megoldások használata, rendszeres hibajavító frissítések és biztonságtudatos felhasználói hozzáállásban

Shannon [redacted]
Dustins first credit card. I'm soooo proud!!!! Your growing up so fast :) —
with Dustin [redacted]



Like · Comment · Share · 3 minutes ago via BlackBerry · [icon]

[blue profile picture] [redacted] thanks for dinner... and my new car and everything on ebay
2 minutes ago · Like

[green profile picture] [redacted] Did you just post some kids credit card number all over Facebook?
about a minute ago · Like

Write a comment...

Shannon [redacted]
um hello everyone I didn't mean to put dustins credit card # on fb so one person yelling at me is enough. thanksss

[icon] Like · Comment · 32 minutes ago via BlackBerry · [icon]

first_credit.png

Mindenkinek meg kell tanulnia nem csak azt, hogy többnyire nem osztunk meg mindent mindenkivel, hanem azt is, hogy vannak kritikus adatok is, amiket sosem. Ilyen a névvel, olvasható kártyaszámmal mutogatott bankkártya is.

Privacy Settings > Profile Information

[Back to Privacy](#)[Preview My Profile...](#)

About me About Me refers to the About Me description in your profile	Everyone
Personal Info Interests, Activities, Favorites	Friends and Networks
Birthday Birth date and Year	Friends of Friends
Religious and Political Views	Friends of Friends
Family and Relationship Family Members, Relationship Status, Interested In, and Looking For	Friends of Friends
Education and Work Schools, Colleges and Workplaces	Friends of Friends
Photos and Videos of Me Photos and Videos you've been tagged in	Friends of Friends
Photo Albums	Edit Settings
Posts by Me Default setting for Status Updates, Links, Notes, Photos, and Videos you post	Everyone
Allow friends to post on my Wall	☒ Friends can post on my Wall
Posts by Friends Control who can see posts by your friends on your profile	Everyone
Comments on Posts Control who can comment on posts you create	Friends of Friends

fbsettings.png

Jó esetben mindenkinek ismernie kellene ezeket. A szülő csak akkor tud érdemben segíteni a gyerekének, ha tisztában van a különféle beállítási, korlátozási lehetőségekkel is.

Ha Aszad nem csatlakozik, visszatérnek a háborúhoz

Lenyilagták, de így is felrobbantotta magát az öngyilkos merénylő

KÜLFÖLD GYILKOSÁG EMBERKÍNÁZÁS NÉMETORSZÁG

Nőket kínozt és gyilkolt meg egy házaspár Németországban



INDEX

2016.05.03. 19:35

Ajánlom 34

Múlt héten fogták el Németországban Wilfred V.-t és Angelika B.-t, akiket azzal gyanúsítanak, hogy embereket kínoztak, majd gyilkoltak meg. **A negyvenes éveikben járó pár társkereső hirdetésekkel cserkészte be áldozatait, akiket aztán elraboltak és különböző kegyetlenkedéseknek vetettek alá, mielőtt kivégezték őket.**

A BBC szerint a pár női tagja már beismerte tettét, a férfi viszont azt mondja a rendőröknek, hogy nem csinált rosszat. A rendőrség közben rábukkant a pár Höxterben található házára, ahol igazi kínozókamrát rendeztek be. A hatóságok egyelőre két nő meggyilkolását kötik az ex-házaspárhoz, de a nyomozást vezető rendőr azt mondta kedden, hogy további áldozatok is előkerülhetnek.

(Borítókép: Höxter városa. Fotó: Alexander Koerner/Getty Images)

tarskereses.jpg

Nem csak a Gyilkos elmék tévésorozatban történhetnek az emberrel rossz dolgok. Európa, Németország, 2016. - társkereső hirdetésekkel csalták törbe áldozataikat, majd a pincéjükben halálra kínozták őket a Höxterben lakó házaspár.



utcaimobil.jpg

Nem tudni, hogy ez még csak egy vicces kép, vagy már maga a valóság. Tény azonban, hogy egyre több az olyan gyalogos, aki zombiként bambul a mobiljára, és emiatt nem figyelnek környezetükre, árkokba esnek, közlekedési baleset áldozatai lesznek, esetleg lezuhannak valahonnan.

ÓRIÁSI BOTRÁNY TÖRT KI EGY GIMNÁZIUMBAN, MIVEL A DIÁKOK EGYMÁS KÖZÖTT CSERÉLGETTÉK A MEZTELEN KÉPEIKET

VELVET 2015.11.10. 10:37

Botrány tört ki egy amerikai iskolában, amikor kiderült, hogy a diákok egymás pucér képeit osztották meg egymás között. Legalább száz gimnazista érintett, és a rendőrség is nyomoz az ügyben. Az résztvevők saját képeiket cserélgették, akár az autókártyákat – írja a *Daily Dot*. A csoport tagjai telefonon keresztül mutogatták a pornográf tartalmakat, és kamu appokkal próbálták titkolni a rendszert, hogy mondjuk úgy tűnjön, a számítógépet nézegetik a pucér osztálytársaik helyett.

A diákok pontokat gyűjtöttek, az lehetett a cél, hogy minél több képet szerezzenek be. Rengetegen csatlakoztak a *sexting-körhöz*, minimum száz tinédzser után nyomoznak. A coloradói iskola dolgozói és a szülők is segítik a rendőrség munkáját. Az már szinte biztos, hogy a gimnázium focicsapata oszlopos tagja lehetett a közösségnek, az utolsó meccsük elmaradt a botrány miatt. Komoly következményei lehetnek az ügynek, amiben legalább 300-400 kiskorúakról készült meztelen kép cserélt gazdát.

[Ajánlom](#) [Facebook](#) [Twitter](#) [Google+](#)

gimnazium.png

Óriási botrány egy középiskolában. A 2015-ös történetben a diákok megosztották egymás meztelen képeit, és a kiskorúakról készített felvételeket úgy cserélgették egymás között, mint máshol a focis vagy kosaras kártyákat. A titkos sexting-körhöz több, mint százan csatlakoztak, végül rendőrségi vizsgálat lett az ügy vége.

APJA PÉNZE SEM MENTI MEG KIRÁLY LINDÁT

2014.03.12. 06:15

Király Linda Baki himnusz letöltés Király Tamás Kisalföld

Király Tamás felvásárolta azoknak a videóknak a jogait, amelyeken lánya, Király Linda évekkal ezelőtt belesült a Himnuszba. A talán már rég elfeledett történetet most újra leporolta a Király család.

A jogszabályokat és a pénzt hívta segítségül Király Tamás, hogy eltüntesse az internetről lánya több mint tíz évvel ezelőtti bémázását. Sokan emlékezhetnek rá, Linda egy kosármeccs alkalmával énekelte a Himnuszt, de elvettette a szöveget. Lehet, a fegyver fordítva sült el, mert Linda és a Himnusz újra napirendre került a világhálón.

A Comment:com ugyanis hozzájutott egy levélhez, amit az apuka az egyik videomegosztó portálhoz juttatott el: „Tisztelt Indavideo, Mi, a Crown Music Bt., mint az alábbi linken található videó 2014. február 4-től online felületeken történő felhasználásának egyedüli jogtulajdonosa, kérjük a videó azonnali eltávolítását az oldalukról. http://indavideo.hu/video/Kiraly_Linda_-_Himnusz Amennyiben kérésünknek nem tesznek eleget, a hatályos jogszabályok alapján jogi útra fogjuk terelni az ügyet. Együttműködésükben bízva, Király Tamás, ügyvezető.”

Ezenkívül a YouTube-ról és GameStar nevű oldalról is eltűnt az eddig sok kattintást hozó felvétel. A Bors megkereste Király Tamást, hogy megkérdezze, miért érezte szükségesnek eltüntetni a kinos videókat az internetről. Ő megkérte lapunk munkatársát, hívja vissza később, de többé nem vette fel a telefont. Szerencsére korábban már beszélt a Borsnak az incidensről, miután Lindának Mága Zoltán jótékonyági koncertjén is meggyűlt a baja a Himnusszal. Többet azt hitték, az énekesnő nem mer kiállni a színpadra, de kiderült, csak egy dalra volt szerződése.



Íme, a három és fél hónappal ezelőtti nyilatkozat: „Ha kellett volna, szívesen ment volna, eleget bántották már őt ezzel, legalább lett volna alkalmunk bizonyítani. Frusztráló, hogy nem hagyják békén ezt a szerencsétlen lányt már nem tudom, mióta, körülbelül tíz éve. Hát esküszöm, itt fel lehet koncolni négy embert és kap az ember hat évet, őt meg tíz éve kínozzák már ezzel. Ez borzasztó, ez szörnyű, ahelyett, hogy örülnének, hogy van egy ilyen tehetség, aki dolgozik és letesz az asztalra dolgokat, egyfolytában bántják. Ráadásul alaptalanul” – magyarázta tavaly november végén a Borsnak.

Lindát is szeretettük volna megkérdezni, mit szól ahhoz, hogy a videók egy része eltűnt, de lapzártánkig őt sem értük el.

Így történt tíz éve a baki

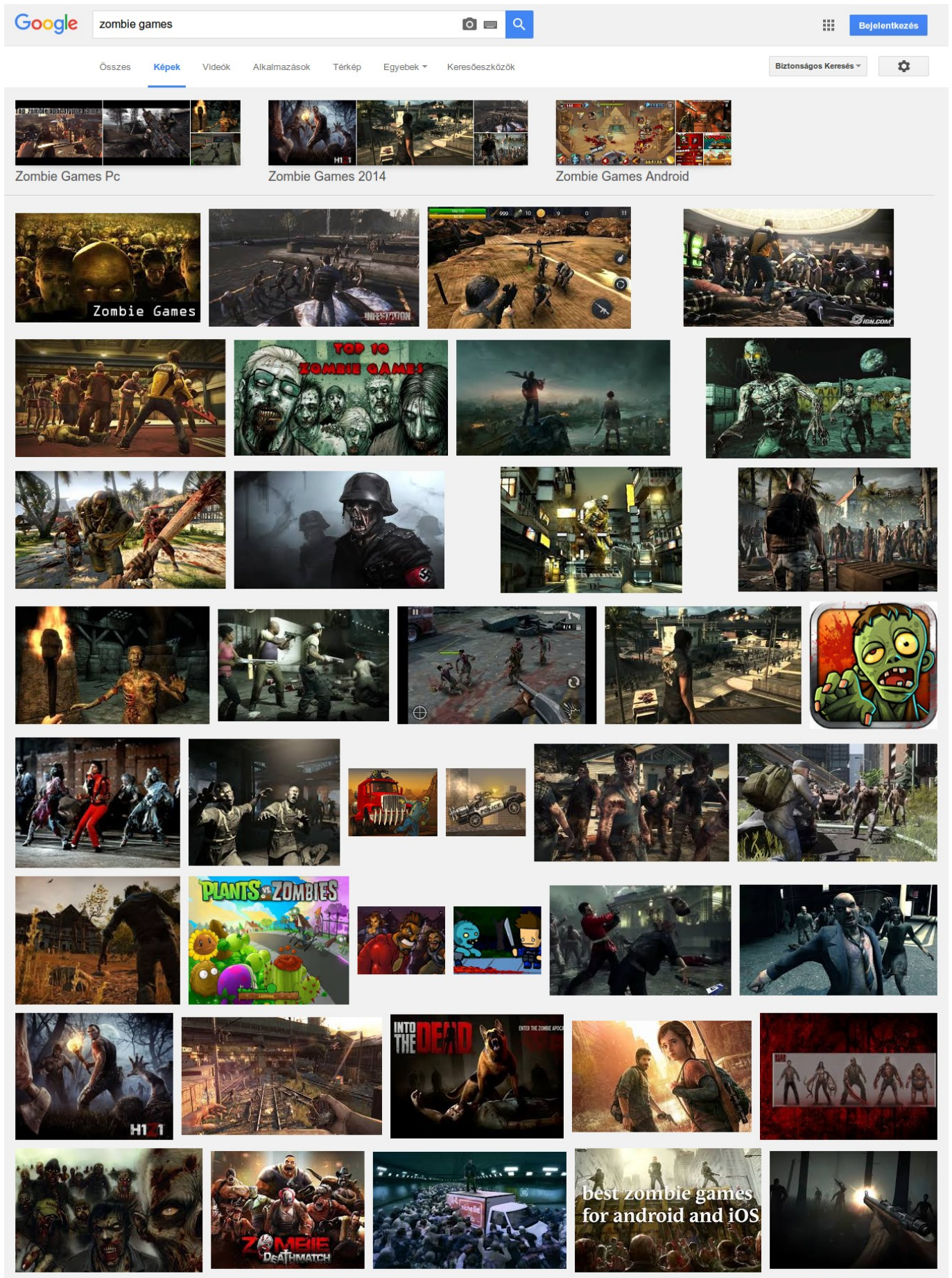
Sikerült megtalálnunk azt a szervezőt, aki meghívta az énekesnőt az ominózus, tíz évvel ezelőtti kosármeccsre. – A közönség először elég türelmesen reagált annak ellenére, hogy Linda belesült a szövegbe. Akkor kezdtek el kifütyülni, amikor arra kérte őket, énekeljenek együtt, hiszen „magyarok vagyunk mindannyian”. Úgy gondolom, ez olaj volt a tűzre, de Linda édesapja profin reagálta le a malört. Beszaladt a lányához és együtt énekeltek el a Himnuszt, ezután már a közönség is elnézőbb volt, azt persze nem tudták, ki az, aki kisegítette az énekesnőt – mesélte el lapunknak a történeteket Tímár András.

Akár milliókba is kerülhet a lépés

El lehet tüntetni bármit is a netről? A Bors szakértőt szólaltatott meg. – A jogi megoldások mellett videofelvétel és képek esetén megoldás lehet azon felhasználók megkeresése, akik a felvételeket feltöltötték és lehet velük egyezkedni, hogy mennyiért adnák el a felvételeket. Ezt nem szoktuk javasolni, mert nem lehet pontosan meghatározni, kinek lehet még a birtokában letöltve egy-egy ilyen videó vagy kép, így az visszakerülhet a netre. Jobb, ha a forrásnál, a szolgáltatónál tiltatjuk le a videót, ami viszont drága eljárás. Félmilliótól akár több tízmillióig is terjedhet az összeg – magyarázta lapunknak dr. Romhányi Gergely, a Repon Consulting and Research Kft. ügyvezetője.

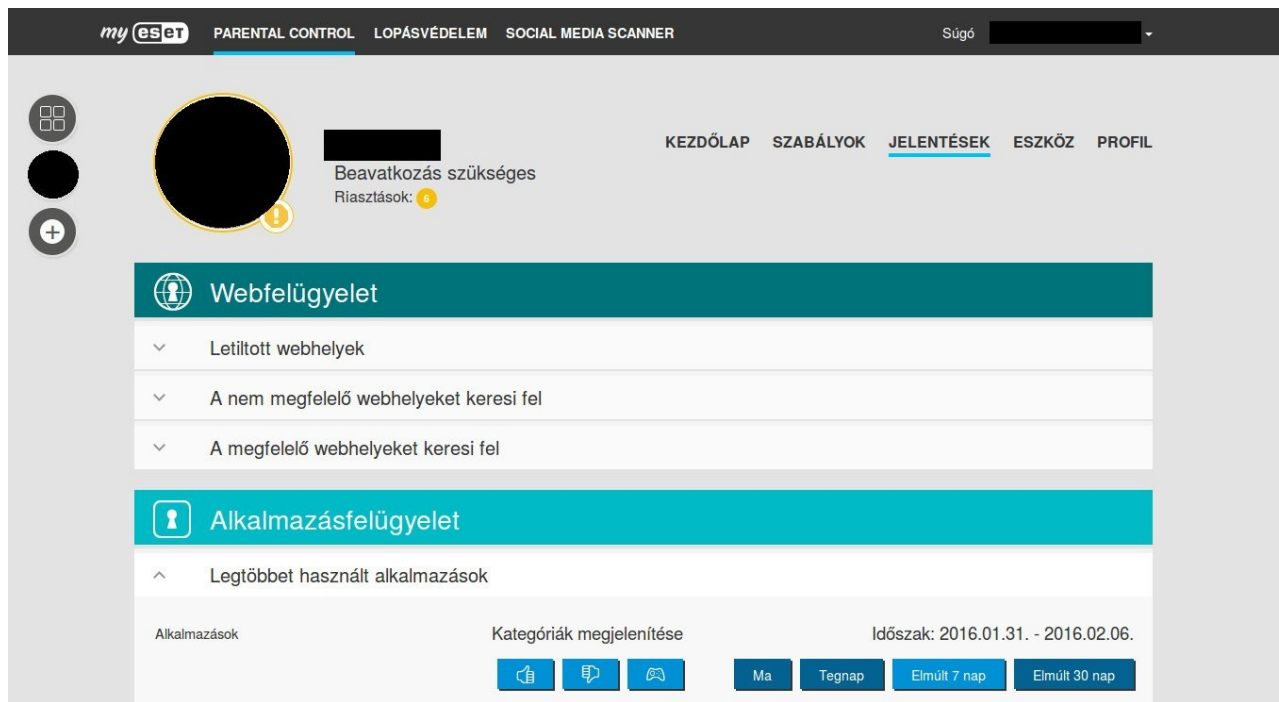
kiraly_apja.png

Az „internet nem felejt” szabályt meg lehet ugyan próbálni erővel, vagy sok pénzzel gyengíteni, ám a próbálkozások sokszor inkább kontraproduktívak, és ezáltal csak még fokozottabb érdeklődést váltanak ki.



zombigames_google.png

Ha a mellékelt keresőszót begépeljük a keresőbe, nagyon durva, erőszakos képek jönnek elő.



eparental.jpg

Léteznek már olyan okostelefonos programok, amely segítségével a szülők távolról, biztonságos szabályoknak megfelelően tudják gyermekük internetes felügyeletét elvégezni. Az ESET Parental Control segítségével emellett időkorlátszabályokat is meghatározhatunk, de a GPS koordináták alapján a tartózkodási helyet is lekérdezhetjük.

Azt mondta, szép vagyok, és ágyba hozza majd a kakaót nekem



KALAS GYÖRGYI

2016.03.03. 12:13



Csavargás, drogozás, prostitúció – sorolják a lányok az esztergomi leánynevelő intézetben, amikor azt kérdezem, miért kerültek ide. Esszük a vacsorát, pörköltös tészta szafttal, savanyú káposztával. Öten ülünk az asztalnál, és az a kép kezd kirajzolódni, miszerint a történet szinte mindenkinél ugyanaz:

11-12 éves korban ismerkedés a drogokkal, főleg herbál, cigibe sodorva. Ötödiktől folyamatos lógás az iskolából, kiemelés a családból, szökések, csavargás, prostitúció.

„Én 12 évesen mehettem haza az intézetből a nagymamámhoz” – kezdi a történetét az egyik 14 éves lány, Brigi, aki két éve van Esztergomban, idén nyáron „szabadul”. Hazagondozása után a Facebookon ismerkedett meg egy 45 éves férfival, aki profilképe alapján bejelöltte, ő meg visszajelöltte, mert nagyon boldog volt, hogy 12 éves létére azt írja neki valaki, hogy milyen szép. Attól kezdve sokat cseteltek, míg a férfi rábeszélte, hogy költözzön hozzá. Brigi éjjel indult el biciklivel.

„Hogy mivel győzött meg? Hát, hogy mellette önálló lehetek. Saját házam és konyhám lehet, azt mondta, mellette én leszek a királynő. És ha akarom, reggel ágyba hozza a kakaót.” Brigit teljesen véletlenül látta meg a bátyja a buszmegállóban, majd a nagymama hívta a rendőröket, akik kimentek arra a címre, amit Brigitvel találkozási pontként megbeszéltek. Ekkor derült ki, hogy a lányt már előre eladták külföldre. A lányt azonnal Esztergomba szállították védelmi okokból.



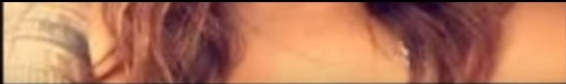
12eves.jpg

A gyermekek jogaival való visszaélésnél a csábítók, a stricik is használnak számítógépet, közösségi oldalakat. Az Index cikke rámutat, az ismerkedő felnőttek eleinte fűt-fát ígérnek, aztán sok esetben szexrabszolgának adják el a behálózott kiskorút.



MEZTELEN KÉPEK | TANÁRNŐ | DIÁK

EZ A TANÁRNŐ MEZTELEN FOTÓKAT KÜLDÖZGETETT MAGÁRÓL A DIÁKJAINAK



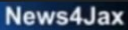
**VIK**

2016.02.01. 15:17

 Ajánlom  2 

A 28 éves Floridai testnevelés-tanárt, bizonyos Dionne Younce-t **felfüggesztették**, miután nyilvánosságra került, hogy olyan képeket küldözgetett magáról a diákjainak, amelyek egyáltalán nem tartoznak a tanári munka hatáskörébe, sőt. Állítólag a fotókon meztelenül pózolt, így nem csoda, hogy a rendőrség vizsgálatot indított ellene.

A tornatanárnőt, aki egyébként az iskola női súlyemelőcsapatának edzője is egyben, jelen pillanatban azzal vádolják, hogy legalább három diákjával viselkedett nem éppen az elvártaknak megfelelően, vagyis szexuális értelemben „illetlenül”. Az Allen D. Nease középiskolában tanuló diákok egyhangúlag állítják, hogy mindannyian rendszeres üzenetváltásban voltak Younce-szal, aki elkezdte követni őket Twitteren, Instagramon és Snapchat-en is. (A **Snapchat** az Instagramhoz hasonló videó- és fotómegosztó alkalmazás okostelefonra.)



A 28 éves tanárnő meztelen fotókat küldözgetett magáról a diákjainak

Az egyik tanuló vallomásaiban hozzátette, hogy a tanárővel folytatott bensőségesnek mondható kapcsolata először enyhe flörttel kezdődött, ami később szexuális értelemben „elharapódzott”, és odáig fajult, hogy meztelen képeket küldözgettek egymásnak.

Négy másik diák mellett – akiknek sem a nevét, sem a korát nem hozták még nyilvánosságra – két főasszisztent is említene a jelentésekben, tehát Younce széleskörű kapcsolatrendszert kívánt kiépíteni erotikus üzenetváltások révén.

florida.jpg

Amire korábban egyáltalán nem kellett számítani, az is megtörténhet. A tanár-diák viszony az interneten még normál esetben sem egyszerű, de itt egy floridai tanárnő saját diákjainak küldözgetett meztelen képeket saját magáról. Lehet, hogy kellene egy jogszabály, amelyben ha tanár, orvos, pap vagy rendőr él vissza a bizalommal, azzal dupla büntetést kockáztassanak.



COMMENT 04.21.16 11:05 PM ET



BEN COLLINS



Hillary PAC Spends \$1 Million to 'Correct' Commenters on Reddit and Facebook

FEC loopholes mean Correct the Record can openly coordinate with Clinton's campaign.



Citing "lessons learned from online engagement with 'Bernie Bros,'" a pro-Hillary Clinton Super PAC is pledging to spend \$1 million to "push back against" users on Twitter, Facebook, Reddit and Instagram.

Correct the Record's "Barrier Breakers" project boasts in a press release that it has already "addressed more than 5,000 people that have personally attacked Hillary Clinton on Twitter." The PAC released this on Thursday.

The PAC was created in May of last year when it was spun off from the American Bridge SuperPAC, which is run by longtime Hillary and Bill Clinton supporter David Brock. Brock also founded the left-wing media watchdog website Media Matters for America.

clinton_bertroll.jpg

Naivság azt gondolni, minden igaz, ami az interneten található. Sőt, egyes emberek, csoportok, cégek jelentős összegeket is hajlandóak áldozni azért, hogy a számukra kényelmetlen kritikákat megpróbálják eljelentékteleníteni, töröltetni, módosítani. A negatív kritikák miatt időnként még percek is indulnak.

⚡ MINDEKÖZBEN TEGNAP



BOLCSÓ DÁNIEL • BESZTÖF

TEGNAP, 00:26

Egyre népszerűbb a csalóóra a brit iskolákban

Nagy-Britanniában egyre inkább divatba jönnek a kifejezetten iskolai csaláshoz árult órák – írja a BBC. Ezeknek a lényege, hogy rájuk lehet tölteni bármilyen szöveget, hogy a dolgozatírás alatt puskázásra tudják használni a diákok. Ha pedig a tanár épp arra kanyarodik, egy gombnyomás, és már csak a hagyományos óralap mutatja ártatlanul az időt.



Még csak nem is arról van szó, hogy az élelmes diákok kitaláltak egy új, kreatív puskázási módszert – maguk a cégek árulják az órákat kifejezetten csaláshoz. Az Amazonon például olyan szövegekkel lehet találkozni a különböző típusoknál, hogy "diák vizsgaóra", vagy egyszerűen "csalóóra", de van olyan is, amely még a félreértés legkisebb esélyét is szeretné kizárni:

” Ezt az órát kifejezetten arra tervezték, hogy egy vizsgán csalni lehessen vele.

Nem csoda, hogy a brit tanárok kiakadtak az új módszeren. A BBC szerint attól tartanak, hogy az órák könnyen csalásra csábíthatják a vizsga miatt stresszes diákokat. Fellépni egyre nehezebb az ilyesmi ellen, mert szinte követhetetlen az egyre újabb csalókötyük megjelenése.

Folyamatosan fejlődő piacról van szó, a 2016-os változat már 4 helyett 8GB memóriával érkezik, bizonyos modelleket pedig már 15 ezer forintnyi összegért meg lehet venni. De ha az óra nem elég kényelmes, különböző típusú csalótollak vagy éppén csalószámológép is beszerezhető.

csaloora.jpg

Már 50 dollárért lehet rendelni az Amazon webáruházból úgynevezett csalóórát, amellyel bármilyen dolgozatot megírhatunk. 4 és 8 GB-os tárolójába rengeteg adat belefér. Sok tanár egyáltalán nincs tisztában az efféle műszaki „vívmányokkal.”

The Local uses cookies.
[More info.](#)
[Got it!](#)

Norway's news in English
Change editions:
[Austria](#) · [Denmark](#) · [France](#) · [Germany](#) · [Italy](#) · [Spain](#) · [Sweden](#) · [Switzerland](#)

THE LOCAL
no

Follow The Local on Twitter
Norway's news in English

Newsletter sign-up
Site search

News & Features ▾
Jobs ▾
Community ▾
More ▾

f
twitter
in
g+

The Local has a new FREE App.
Keep in touch with what's going on around Europe.

OPEN

National

2,302
jobs available

Several rape crisis centres report an increase in the number of women attacked by men they met on Tinder. Photo: Gorm Kallestad/NTB Scanpix

Norway sees more rapes tied to Tinder use

Published: 19 Feb 2016 11:13 GMT+01:00

Share
Tweet
+ Share
reddit

Both police and numerous rape crisis centres say they have noticed an increase in the number of women subjected to sexual attack after having met someone through online dating or apps like Tinder.

- **'No means no': Norway sends migrants on anti-rape courses** (20 Jan 16)
- **Norway woman makes film about own rape** (16 May 15)

"We began seeing a significant increase last year in the category that includes rapes after initial contact was made on Tinder or other dating sites," Oslo Police spokeswoman Kari-Janne Lid told VG.

In 2014, 29 percent of all reported rapes in Oslo fell in that category. Last year, the number was up to 40 percent.

Ann Helen Lomsdalen, who leads a sexual attack centre in Frederikstad, has warned area women about the naive use of Tinder.

"We are seeing more rapes in connection with Tinder dates. It is a trend that I think is frightening. It has happened a lot in the eight years I have led the centre," she told VG.

Three out of the nine cases the centre has handled this year involve women assaulted by Tinder connections.

"That in itself maybe isn't a huge number, but there is a pattern emerging," she said.

Story continues below...

Most read
Most comments

- Oslo is the real 'Capital of Scandinavia'
- Norway's tough asylum plans face resistance
- Norway updates cross-border child welfare guidelines
- Seven arrested after Oslo pub shooting
- Bruce Springsteen gig confirmed in Norway

Sponsored Article
US taxes and FATCA: 'The time for hiding is over'

National
Norway police to go back to being unarmed

You May Like
Sponsored Links

norway.jpg

Norvégiában a rendőrség azt észlelte, hogy amióta elterjedt a Tinder, azóta nőtt azoknak a nőknek a száma, akik megerőszakolóikkal randioldalakon, illetve randi appokon keresztül ismerkedtek meg. Az ilyen esetek aránya 2014-ben 29% volt, míg 2015-ben már 40 százalékra emelkedett. A randi alkalmazások kínálata az erőszakolók számára olyanok, mint egy étlap.

Felgyújtotta magát egy 12 éves fiú



KOVÁCS M. DÁVID

2016.05.26. 23:45

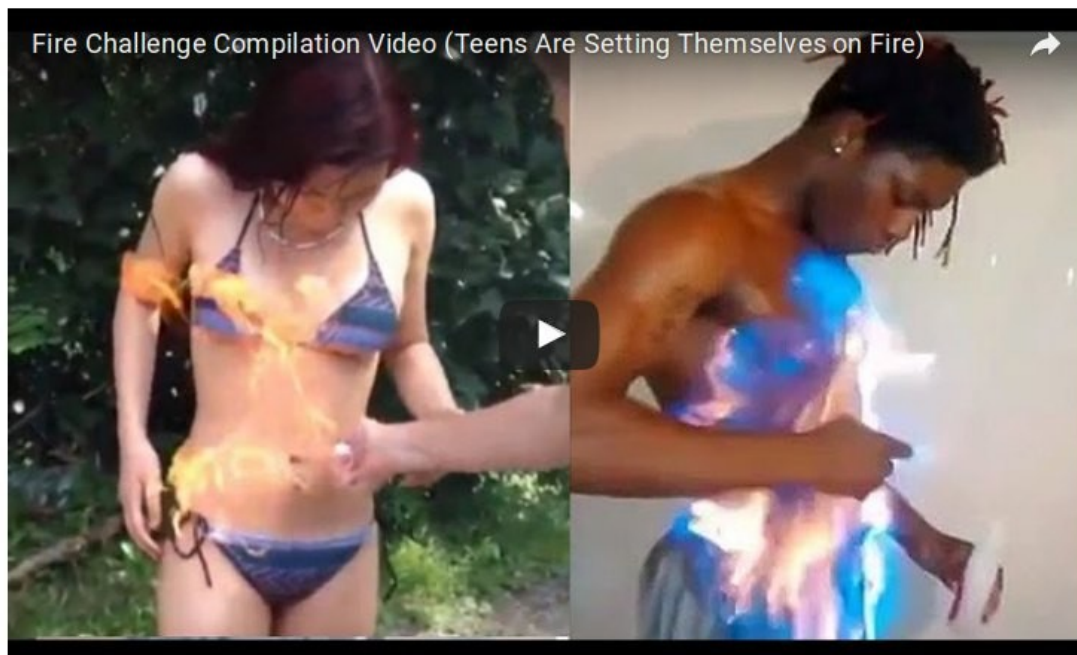
Ajánlom 38

Egy ostoba internetes trend áldozata lett egy 12 éves fiú New Yorkban, aki fürdőszobájukban gyúlékony folyadékkal locsolta le testét, majd gyufát gyújtott, és begyújtotta magát.

A tűzoltókat helyi idő szerint kedd éjjel riasztották egy queensi lakáshoz, ahol tüzet ugyan nem találtak, csak egy súlyos égési sérüléseket szenvedő fiút, írja az [Associated Press](#).

A fiút súlyos égési sérülésekkel szállították kórházba. A rendőrség közleménye szerint valószínűleg túléli majd a balesetet. Úgy tudják, a tüzet a szomszédok segítettek eloltani, miután a kisfiú lángokba borulva kirohant a házból.

A "fire challenge" elterjedése egy ideje már komolyan aggasztja az amerikai közvéleményt. Nem ez az első alkalom, amikor balul sül el a mutatvány:



fire_challenge.jpg

A "fire challenge" nevű ostoba internetes trend terjedése elég aggasztó a szülők számára. Korábban is voltak már ebből balesetek, legutóbb egy 12 esztendős amerikai fiú szenvedett súlyos égési sérüléseket, mikor a fürdőszobában gyúlékony folyadékot locsolt magára és meggyújtotta.



HIREKET MONDUNK | PAKISZTÁN | EGYENJOGUSÁG

FELGYÚJTOTTA A SAJÁT LÁNYÁT, MERT AZ ENGEDÉLYE NÉLKÜL HÁZASODOTT



GYULAI BENCE

 KÖVETÉS

2016.06.10. 16:27

f Ajánlom 35

Tegnap járta körbe a világot – **a CNN tudósítása** nyomán – annak a pakisztáni anyának **a híre**, aki ágyhoz kötözte és felgyújtotta a saját lányát, mert a lány engedély nélkül férjhez ment a szerelméhez. A 18 éves lány megbüntetésében a lány testvére is segédkezett, ő továbbra is szabadlábban van valahol, míg anyját, Parveen Bibet elfogta a rendőrség. Mára fotók is érkeztek a történethez, és további részleteket olvashat alább.

Lahor egy Magyarországnál több lakosú város Pakisztánban. Itt élt a 18 éves Zeenat Rafique szüleivel és a testvérével. A lány azzal vívta ki a család haragját, hogy beleszeretett egy volt iskolatársába, Hassan Khanba, aki most 19 éves és autószerelő. A pár még a suliban jött össze, és öt évnyi szerelem után 2016. május 29-én összeházasodtak egy polgári szertartással, majd össze is költöztek, tisztes távolban a menyasszonyok szüleitől.



Kicsit elvárjuk, hogy Budapestet a világon mindenhol ismerjék. Na de ön ismeri ezeket a városokat?

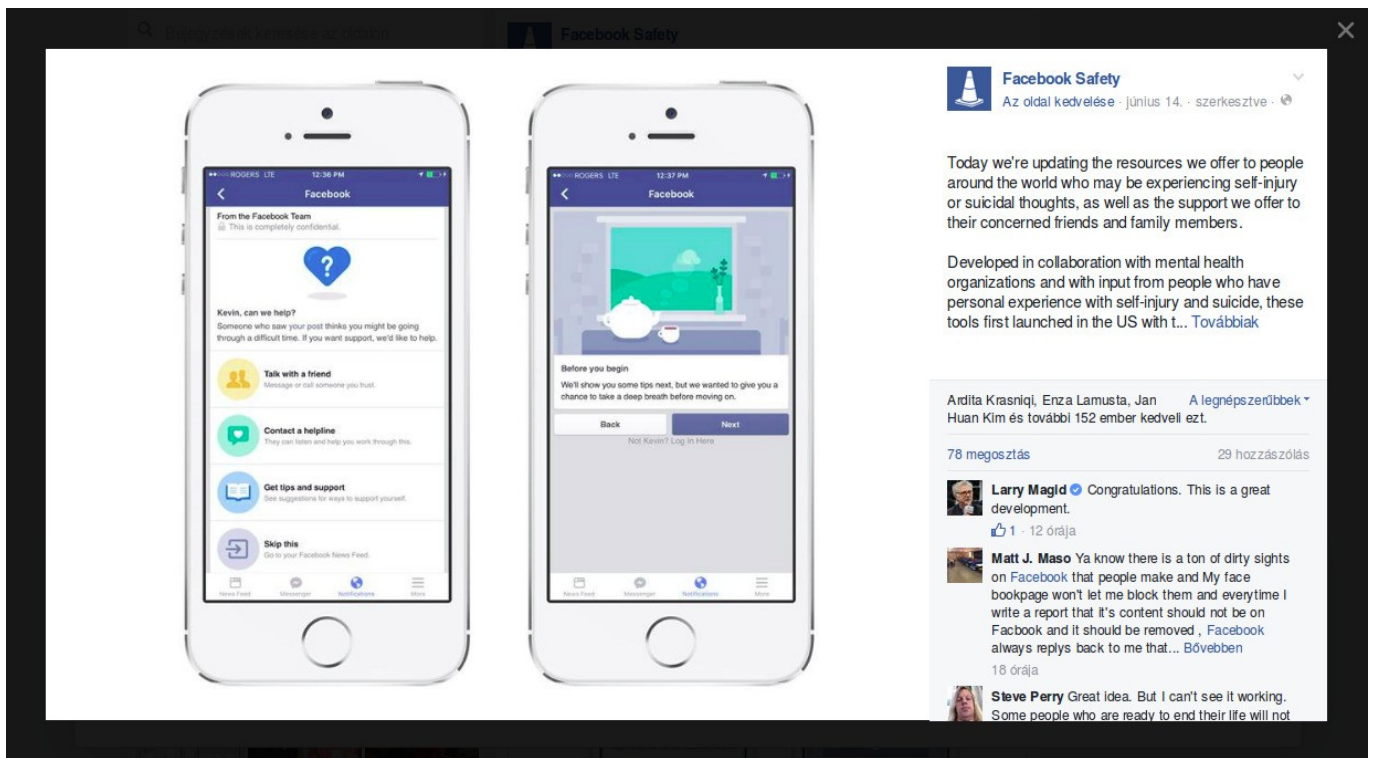


Northfoto



maskultura.jpg

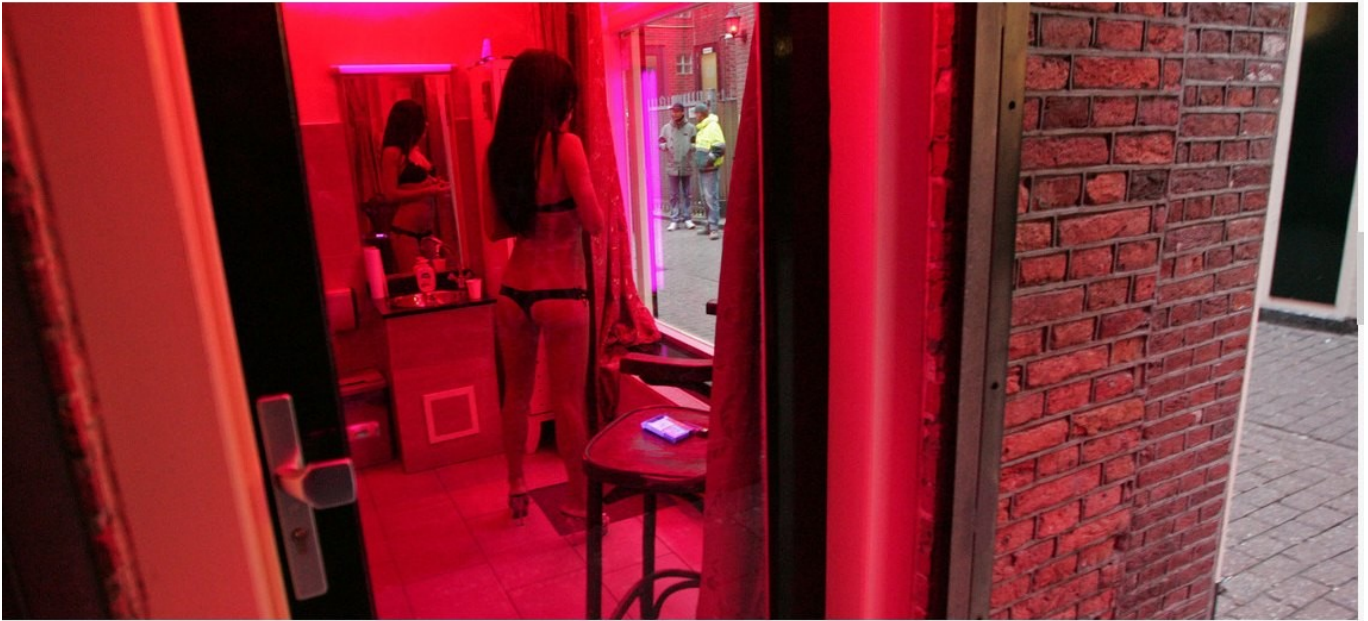
Az interneten még magyarul is könnyen botlunk olyan felkavaró, ijesztő tartalomba, amely a közép-európai keresztény kultúrkör értékrendjéhez képes egészen abszurd szokásokat, eltérő kultúrát mutat. Pakisztánban egy anya megölte a saját lányát, mert az ősi szokások ellenére engedély nélkül és rangon alul ment férjhez.



fb_ongyilkossag.jpg

2016. júniusban egy új lehetőség került a Facebook-ba. A közösségi oldalon mostantól névtelenül jelenthetjük, ha ismerőseinknél esetleg öngyilkosságra utaló bejegyzést, üzeneteket látunk.

Egyre több magyar lesz szexrabszolga



-DA-

KÖVETÉS

2016.02.20. 07:30

Ajánlom

155



Egyre több magyar fiatal esik áldozatául az emberkereskedelemnek. Jellemzően a három, anyagilag a leghátrányosabb helyzetben lévő megyéből adják vagy rabolják el szexrabszolgának a 14–23 éves lányokat és fiúkat, akiket Nyugat-Európában dolgoztatnak – írja a Magyar Nemzet az ökömenikus pedagógusműhely rendezvényén elhangzottak alapján.

Az Europol statisztikája megdöbbentő:

minden ötödik áldozata magyar volt az európai emberkereskedőknek 2009 és 2013 között.

Visszonyításként: az Európai Bizottság megállapította, 2010–2012-ben az EU-ban 30 146 áldozatot vettek nyilvántartásba. Különösen aggasztó, hogy évről évre nő a szexuális célú kizsákmányolás az emberkereskedők áldozatai között - írja a lap.

A Sándor kör csütörtöki előadásán az is kiderült, hogy

Magyarország a szexuális célú emberkereskedelem kiinduló országa lett.

14–23 éves lányokat és fiúkat adnak vagy rabolnak el, illetve kecsegtető jövőképpel csábítanak Nyugat-Európába. Olyan országokba viszik az áldozatokat, ahol csak a futtatás tiltott. Így Németországba, Ausztriába, Belgiumba, Hollandiába, az Egyesült Királyságba, Franciaországba, Svájcba és Olaszországba szállítják a fiatalokat, hogy ott három műszakban, heti hét napon át prostitúcióra kényszerítsék őket. Az emberkereskedők jellemzően Borsod-Abaúj-Zemplén, Szabolcs-Szatmár-Bereg és Baranya megyéből, a mélyszegénységben élő, főleg roma populációból szedik áldozataikat.

Az is egyre többször fordul elő, hogy a nyomorban élő családok adják el gyermekeiket, hogy az itthon maradottak meg tudjanak élni.

emberkereskedelem.jpg

Egyre több fiatal esik áldozatul az emberkereskedelemnek, az ismerkedéssel vagy hamis álláshirdetéssel kezdődő netes üzenetváltások után szexrabszolgaként adják el a fiatakorúakat.

A tinédzsereket féltik a hatóságok az élő videózás terjedése miatt



BOLCSÓ DÁNIEL

KÖVETÉS

2016.04.14. 15:38



A norvég rendőrség egy veszélyes új közösségi médiás trendre **figyelmeztette** a norvég szülőket: a tinédzserek élő videóközvetítést adnak magukról, és ezeket Facebook-csoportokba posztolják, ahol akár több ezer csoporttag láthatja és kommentelheti az élő adást.

A rendőrség szerint ennek a trendnek az oka az a frissítés, amely lehetővé tette, hogy a Facebook Live nevű szolgáltatással bárki bármilyen csoportban élő közvetítést sugározzon a közösségi oldalon. Ez persze eddig is megoldható volt más platformokon, de a Facebook méretes felhasználói bázisával a potenciális visszaélések száma is növekszik.

Maguk a videók általában teljesen ártatlanul indulnak, a nézők kommentjei viszont gyakran viszik el a videóban szereplő számára kellemetlen irányba az eseményeket. A rendőrség attól tart, hogy ezek a közvetítések a melegágyai lehetnek a cyberbullyingnak, vagyis a már az offline világban is rengeteg problémát okozó zaklatás netes formájának. Az online zaklatás az utóbbi évek egyik legkomolyabb veszélye a kiskorúakra, mert a szülőknek vagy tanároknak gyakran még kevesebb a kontrolljuk, mint a személyes iskolai szituációknál, és sok esetben kevésbé is értik a tinédzserek által rutinszerűen használt online felületek működését.

facebookvideo.jpg

Egy újítás, aminek beláthatatlan következményei vannak: már realtime, élő videókat is megoszthatunk a Facebook közösségi oldalán, és sajnos volt már rá példa, hogy egy nő öngyilkosságát lehetett figyelemmel követni, illetve egy tinédzser barátja nemi erőszakát is közvetítette ily módon.

Fogvatartott és szexre kényszerített 14 éves lányokat egy hajdúhadházi férfi



Tbg · BÜNYÜGY · ma 10:46 · 0 · 85

Elkészült a vádemelési javaslat az ellen a férfi ellen, aki a gyanú szerint prostituáltként dolgoztatott gyermekkorú lányokat 2010 és 2014 között.

A gyanúsított 2010 októberében egy 14 éves kislányt, valamint 2013 áprilisában egy szintén 14 éves kislányt bezárt a hajdúhadházi házába, ahol bántalmazta és közösülésre kényszerítette őket.

H. Lajos a két sértettet többször arra is kényszerítette, hogy prostituáltként dolgozzanak Debrecenben, majd a férfi a pénzt elvette tőlük.

Az egyik lány 2014. április 27-én a férfi házából el akart menni, azonban ezt H. Lajos nem engedte, a fiatal lányt megverte és bezárt egy szobába. A sértett 2014. májusban azonban meg tudott szökni a férfi házából.

A lány azonban 2014. december 30-án este Debrecen, Petőfi téri Nagyállomáson véletlenül összetalálkozott a férfival, aki nem engedte felszállni a vonatra, visszahúzta, ütlegelte.

A vasúti ellenőrök rászóltak a férfira, így a lány el tudott szaladni a helyszínről.

Az esetről történt feljelentést követően a rendőrök felkeresték a 26 éves férfit, és elfogták.

A rendőrség a gyanúsítottal szemben folytatott nyomozást a napokban fejezte be. (Police.hu)

MŰSORVEZETŐK



Tbg

Merkel szigorítana a német migrációs politikán



Az a menedékkérő, aki bűncselekményt követett el, nem kaphatna menedéket Németországban.

Tovább



Tbg · MIGRÁCIÓ
ma 14:22 · 0 · 25

Az USA szerint az orosz

20160109_fogvatarto.jpg

Sajnos magyarországi példák is vannak, hogy akaratuk ellenére fogvatartanak és prostitúcióra kényszerítenek gyerekkorú lányokat.

Technology

Android

Smartphone Malware Secretly Creates 3D Models of Your Surroundings



By David Gilbert

October 1, 2012 14:57 BST



A university experiment has proven that mobile malware can be used by your smartphone to remotely map the interior of your house or office.



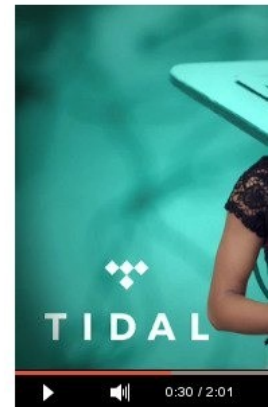
Until now, the idea that your smartphone's camera could be used to secretly build a 3D model of your home or office, upload the data to a remote server, and allow them to virtually snoop around your home, was the preserve of works of science fiction and fantasy.

Reconnaissance



Individual images are uploaded and in combination with the location and orientation data from your smartphone's sensors, they are converted into a navigable 3D model.

IBT VIDEO



Tidal one year on: Has been a success or fail

COLUMNISTS



Rob L. Wagner

Barack Obama and the Saudi Arabia - but they w

READ MORE



2012_3d_android_malware.jpg

Már 2012-ben bemutatták azt a kártevőt, amely az okostelefon kamerájának véletlenszerű időközönként és titokban készített képeiből a szobabelső 3D modelljét is képes volt elkészíteni.

Pucér szelfik csináltak szexuális bűnözőt két amerikai kamaszból

INDEX

2015.09.21. 00:03



Őrült, a lap által idézett szakértők által is nevetségesnek nevezett amerikai jogesetről írt [cikket a Guardian](#): saját magukról készített meztelen fotók miatt került komoly bajba egy amerikai, észak-karolinai kamasz pár. A képeket akkor fedezték fel a hatóságok, amikor a pár iskolájában vizsgálat indult olyan pucér fotók miatt, amelyeket az érintett diákok engedélye nélkül terjesztettek a többiek. Ebben az ügyben a pár mindkét tagja ártatlan volt, viszont a telefonjaikat átnézve megtalálták a róluk készült fotókat.

A most 17, a képek felfedezésének idején 16 éves fiúnak négy képe volt saját magáról, egy ötödik pedig a szintén 16 éves barátnőjéről. A lánynak a saját telefonján csak saját magáról voltak pucér fotói.

Mindkettejüket kiskorú szexuális kihasználásával vádolták meg: egyszerre kezelték őket nagykorúsítva elkövetőként és kiskorú áldozatként, saját maguk kiskorú áldozataként. Mindezt úgy, hogy egyébként ráadásul a szex közöttük nem is volt illegális, mert Észak-Karolinában 16 év a beleegyezési korhatár.

Végül vádalkuval tudták csak elkerülni, hogy börtönbe kerüljenek vagy szexuális bűnözőként regisztrálják őket. A lány júliusban egyezett bele a feltételekbe: egy évre próbára bocsátották, meg kell fizenie 200 dollár büntügyi költséget, tartózkodnia kell a drogtól és az alkoholtól, nem maradhat ki az iskolából, 30 óra közösségi munkát kell végeznie, órákat kell hallgatnia a helyes döntéshozatalról, és egy évig nem lehet mobiltelefonja.

Szeptemberben a fiú, akit az ügy miatt az iskolai focicsapatból is felfüggesztettek, szintén belement egy hasonló vádalkuba: neki egy éven keresztül azt is tőnie kell, hogy előzetes figyelmeztetés nélkül átkutassák. Ha gond nélkül letelik az egy év, akkor az alku részeként törölni fogják őket a büntügyi nyilvántartásból.



Napi.hu-konferencia

NOGUCHI | PORTE
NOVELL

október 1.

AZ ÖTLETTŐL AZ ÜZLETI SIKERIG 20

A kutatás-fejlesztés és innováció hazai
versenypályázati rendszerének megújításáról

▲ hirdetés

▲ hirdetés

pucer_selfie.png

A törvény szó szerinti előírása alapján minden 18 évesnél fiatalabb személyről készített, illetve birtokolt meztelen fotó illegális. Így extrém esetben a szerelmes párként élő tinédzsereket akár szexuális bűnelkövetéssel is megvádolhatják.

Search

Q

[Join Now](#)
[Sign In](#)

CATEGORIES

[News](#)
[Startups](#)
[Top Stories](#)
[Featured Stories](#)
[Founder Stories](#)
[Ask Me Anything](#)
[Lists](#)
[More](#)

DATABASE

[Find Startups](#)
[Find Investors](#)

TIA CONFERENCE

[Jakarta 2015](#)
[Singapore 2016](#)

C. Custer

10:30 am on Jul 9, 2014

ASIA

GAMING

Chinese couple sells their children to traffickers, uses the money to buy in-game items

0 Comments

f

4

t

in

F

Free-to-play games are all the rage in China, but Chinese gamers often shell out a small fortune for in-game items in their favorite games, like weapons and armor. But a young couple in China took things way too far when they sold their two sons to child traffickers and used the proceeds to buy stuff in online games.

The parents in question are A Hui and A Mei (not their full names), a young, unwed couple from China's post-90s generation. In a television interview on Guangdong TV conducted from a local detention center, they revealed that their first child was not planned, and A Mei said that A Hui had no intention of supporting the child financially. Instead, to avoid the financial burden, they sold him to Fujian-based child traffickers.

(See: [Korean father suffocates his crying son, abandons body to play games.](#))

But then, A Mei got pregnant again. "[A Hui] likes buying items in online games, and he likes staying out all night at internet cafes," A Mei told reporters. So many of their collective resources were going into A Hui's gaming that the two felt, again, that they wouldn't be able to support the child. So, once again, they sold him to traffickers.

Child trafficking is a serious problem in China that affects thousands of people every year (full disclosure: a few years ago I made [a documentary film](#) about child trafficking in China). Traffickers sell children to new parents, to street gangs and street peddlers, and even to orphanages for adoption overseas.

(See: [Parents: THIS is how you deal with your child playing too many video games](#))

Trafficking is highly illegal, of course—convicted child traffickers often face execution—and parents who sell children to traffickers are also violating the law. A Hui's father, who was aware of what the couple were doing with their kids, finally reported the problem to police, and both A Hui and A Mei were arrested. The two are now in jail awaiting trial and sentencing for the crime of selling children.

(via [Sina Games](#))

Submit a post

FEATURED

OnePlus X review: the best bang for your buck?

By C. Custer

15 new startup unicorns that emerged in 2015

By Steven Millward

Why Asia's Silicon Valley is in India, not China

By Terence Lee

UberChopper gave regular Jakartans a taste of the lives of the super-rich

By Nadine Freischlad

Read Next

Xbox One preorders begin in China July 31, pricing still a mystery

RECENT COMMENTS

Asia's tech community is not what you assume

Holly, sounds like a great idea for a post, and I know where you can find a free survey tool to get this data ;)

Eli Schwartz - 7s ago

Garena's Shopee could be on its way to beating Carousell in Asia

I'm a seller in multiple platforms. (Carousell, Qoo10, Lazada, etc...) Each of course has its strength and weaknesses. Shopee has provided me some bene...

Jimmy Dewen - 1m ago

Asia's tech community is not what you assume

Leslie, you are correct. Here's a link to see how the answers differed by how much money people want: <https://www.surveymonkey.com/results/SM-B2V2V38J...>

Eli Schwartz - 2m ago

Meet the Indian startup that's making sports fun again

Would you like to download a recreational...

...

ABOUT US · EVENTS · ETHICS · JOIN US · CULTURE · RSS · CONTACT US

COPYRIGHT © 2015 TECH IN ASIA. ALL RIGHTS RESERVED.

FOLLOW TECH IN ASIA

f

t

g

in

YouTube

mixpanel

MOBILE ANALYTICS

techinasia.com.png

A függőségnek időnként sajnos vannak ijesztően szélsőséges esetei is, 2014-ben egy kínai pár eladta saját gyermekeit, hogy a kapott pénzből extrákat vásárolhassanak a kedvenc online számítógépes játékokhoz.

A TWITTEREN STREAMELTE BARÁTNŐJE MEGERŐSZAKOLÁSÁT EGY 18 ÉVES LÁNY



VELVET

2016.04.14. 19:58

Ajánlom

A 18 éves Ohioi Marina Lonina nem csak tétlenül nézte, ahogy barátja Raymond Gates megerőszakol egy 17 éves lányt, de az erőszakot a Twitter videós applikációján, a Periscope-on is megosztotta, így bárki élőben nézhette a dolgot, írja a BBC.



Marina Lonina

Az eset február 27-én történt, ám csak most tett valaki bejelentést a rendőrségen a szemtanúk közül.

A *Daily Mail* szerint az áldozat Lonina barátja volt, és bulizni ment fel a pár lakására. Loninát a szexuális erőszak, emberrablás és kiskorú ellen elkövetett szexuális erőszak segítése mellett azzal is vádolják, hogy meztelen képet készített a kiskorú lányról, az erőszakot megelőző este.



Raymond Gates, az erőszaktevő

Ügyvédje azt nyilatkozta, Lonina kategorikusan tagadja, hogy bűnös lenne. Barátját nem erőszakkal vádolják, az ő vallomásáról még nincs információ.

twitteroszak.jpg

Számos esetben azt tapasztaljuk, hogy a fejlett számítógépes tudás mellett hiányzik az empátia, a megfelelő erkölcsi érzék, együttérzés. 2016-ban egy amerikai lány nem csak tétlenül nézte, hogy barátja megerőszakol egy 17 éves lányt, hanem erről videót is készített a telefonjával, amit megosztott az interneten.

How a Canadian Sikh was photoshopped to look like a Paris attacker

3.5k
SHARES

1944 1434 19 117 0
Share Tweet Share

WHAT'S THIS?



IMAGE: GRASSWIRE FACT CHECK



BY SONAM
JOSHI
INDIA

2015-11-16
07:27:30 UTC

On Saturday, Veerender Jubbal woke up to a social media nightmare. The Canadian Sikh discovered that a photoshopped version of his bathroom mirror selfie was circulating on social media as a photograph of one of the terrorists behind the Paris attacks.

SEE ALSO: [Hate crime charges in beating of Sikh man in Chicago suburb](#)

Jubbal soon took to Twitter to clarify the misunderstanding.

People are editing, and photoshopping my selfies as if I am one of the people causing the issues/problems in Paris.

— Veerender Jubbal (@Veerer_Jubbal) November 14, 2015

Has spread to the point, where many people have had to tweet about the photos being photoshopped..

Any support/nice messages are welcome.

— Veerender Jubbal (@Veerer_Jubbal) November 14, 2015

The controversy grew on Sunday morning, when the photoshopped image was printed on the front page of one of Spain's biggest newspapers *La Razon* and captioned "one of the terrorists". It later apologised for the misunderstanding.

Lo primero, como cada día, nuestra portada <https://t.co/RNwPb8iyI9pic.twitter.com/WW6vQrQnOs>

— La Razón (@larazon_es) November 15, 2015

The picture was also tweeted by the Italian TV channel Sky TG 24.

L'Isis ha inviato una foto dei presunti #kamikaze. <https://t.co/cDqTVIDB0vpic.twitter.com/MEArKimoSb>

— Sky TG24 (@SkyTG24) November 14, 2015

photoshop.png

A sokszor emlegetett tény, hogy amit az interneten látunk, korántsem biztos hogy igaz. Egy Photoshop-pal készült látványos manipuláció, amelyen egy ártalmatlan kanadai szikh férfiből a rajzprogram terrorista merénylőt farag.

Angliában a gyerekek kevesebb időt töltenek a szabadban, mint a rabok



MG

+ KÖVETÉS

2016.03.25. 14:36

Ajánlom

337



Elképesztő eredményre jutott egy országos brit felmérés – írja a **Guardian**. A kutatók azt vizsgálták, hogy mennyi időt töltenek a gyerekek a parkokban, erdőkben, réteken, tehát a szabad ég alatt, és miért. Az országsszerte megkérdezett kétezzer, 5–12 éves kor közötti gyereket nevelő szülő beszámolója szerint a gyerekek 64 százaléka kevesebb mint egy órát játszik naponta a szabadban: ennél az elítélt rabok számára kötelezően előírt szabadtéri tartózkodás is több.

A gyerekek ötöde egy átlagos napon egyáltalán nem tölt időt a szabadban. Egy korábbi, februári kutatás szerint kilenc gyerek közül több mint egy legalább egy éve egyáltalán nem járt parkban vagy a természetben. Az ENSZ ajánlása szerint az iskolás korú gyerekeknek legalább napi egy órát kéne a szabadban játszaniuk.

A kutatók a jelenség okai között a szülők félelmeit, a megfelelő zöldterületek hiányát és az elektronikus kütyük jelentette csábítást sorolták fel. A csökkenő szabadtéri aktivitás hozzájárul a gyerekek elhízásához, és rontja a mentális állapotukat. A gyerekek kétszer annyi időt töltenek a képernyők előtt, mint odakint.



Europress / Getty

Fotó: Matt Cardy / Europress / Getty

A brit kormány most a nemzeti parkokkal karöltve lépéseket tervez, hogy növeljék az iskolások által a szabadban töltött időt.

rabok.jpg

A Guardian megdöbbenő cikke szerint a kütyükbe temetkezett gyerekek már kevesebb időt töltenek a szabadban - erdőn, mezőn, játszótéren, parkban, sportpályán - mint a börtönben ülő elítélt rabok.

ITTHON

Iszlám Állam-szerű kivégzést játszottak egy autista gyerekekkel egy iskolában

KOVÁCS NOÉMI | 2016.05.30. 12:21

Ajánlom 1,3 ezer Tweet G+1 12

Két 13 év körüli gyerek letérdepeltetett egy autista gyereket, állítólag zsákot húztak a fejére, és azt játszották, hogy kivégzik. Az igazgató ugyanezzel a módszerrel büntette meg őket, ezért leváltották.



Képünk illusztráció
Forrás: Dreamstime

Az eset az egyik budapesti általános iskolában történt még decemberben. Két felsős, 13 év körüli gyerek megalázta egy autista társát a szünetben. Azt játszották, hogy

az autista gyerek az áldozat, ők pedig a terroristák.

Az Iszlám Állam rendszeresen tesz közzé az interneten olyan videókat, amelyeken fejükre húzott zsákkal láthatók túsok, letérdepeltetik, aztán kivégzik őket. Ugyanezt játszotta el a két 13 éves gyerek: iskolatársuknak

le kellett térdepelnie, és zsákot húztak a fejére.

Amikor az iskola igazgatója meghallotta, mi történt, behívatta magához a két gyereket, és ugyanazt tette velük, mint amit ők iskolatársukkal.

▼ MOST

22:03 Játssza el: ön is lehet híres sztárszakács!

21:32 Gyurcsány nem fogja össze a Jobbikkal

▶ TOP LIKE

TOVÁBBI ITTHON



Házak égtek ki a villámok miatt



Schiffer András kiszáll a politika élvonalából



Magyarország 2050: egy jó hír érkezett

iszlam_allam.jpg

2016. Magyarország, egy iskolában két gyerek kivégzéssel játszott el autista osztálytársukkal: az áldozatnak le kellett térdelni, zsákot húztak a fejére, és játékból lelőtték. A folyamatos vizuális információk teljesen megváltoztatják az életünket, és ez sajnos óriási hatással van gyermekeink viselkedésére.

Tavaly 5835 kiskorú menekült tűnt el Németországban

TEG

2016.04.11. 18:17

Ajánlom 4

A német szövetségi belügyminisztérium a parlament (Bundestag) megkeresésére adott válaszában azt írta, hogy 2015-ben 8006 kiskorú menekült tűnt el, és közülük 2171 került elő. Így jelenleg 5835 felnőtt kísérő nélküli kiskorú menekültet tartanak nyilván eltűntként, köztük 555 gyereket. Többségük Afganisztánból, Szíriából, Eritreából, Marokkóból és Algériából érkezett.

Az ellenzéki Zöldek szerint "szomorú, hogy a kormány nincsriadókészültségben" annak láttán, hogy csaknem hatezer kiskorú hollétéről nem tudni semmit, írja az MTI. Ez a hozzáállás a védelemre szoruló emberek legsérülékenyebb csoportjához újabb példája annak a "hidegszívűségnek", amellyel a kormány nemrégiben korlátozta a családdegysítési jogot - mondta Luise Amstberg, a Zöldek frakciójának menekültügyi szóvivője. Hozzátette: aggasztó, hogy a kormány nem veszi komolyan a prostitúcióra kényszerítés és a kizsákmányolás egyéb formáinak veszélyét, amely az eltűnt kiskorúakat fenyegeti.



Europress / Getty

Fotó: Alexander Koerner / Europress / Getty

Az európai rendőri együttműködési szervezet (Europol) januárban megjelent becslései szerint több mint tízezer, kísérő nélkül útra kelt kiskorú menekült tűnt el Európában az utóbbi másfél-két évben, minden második Olaszországban. Az Europol szerint valószínűleg nem mindegyikük került bűnözők markába, biztosan vannak olyanok is, akik megtalálták családjukat.

A német szövetségi belügyminisztérium szerint az eltűnt felnőtt kísérő nélküli menekültek tényleges száma jelentősen alacsonyabb lehet, mint a róluk készülő statisztikában szereplő szám. Ennek az az oka, hogy a gyámügyi intézményrendszer gondozza őket, és ezeknek az intézményeknek jogszabályi kötelezettségük bejelentést tenni, amikor eltűnik valamely gondozottjuk, a menekültekkel szerzett tapasztalatok pedig azt mutatják, hogy a felnőtt kísérő nélkül érkező kiskorúak hosszabb távon rendszerint nem a gondozásukra hivatott intézményeknél keresnek védelmet, hanem Németországban vagy Európában máshol élő rokonaikhoz igyekeznek, és amikor megérkeznek, senki nem tesz bejelentést arról, hogy az elvesztésként számon tartott kiskorú megkerült - fejtette ki Johannes Dimroth, a tárca szóvivője hétfőn Berlinben.

nemet_eltunes.jpg

Tömeges a kiskorú menekültek eltűnése Németországban. Az aggasztó statisztikai adat azt mutatja, hogy 2015-ben kis híján hatezer bevándorló gyereknek veszett nyoma, és sajnos közülük sokan vélhetően valamilyen prostitúcióra kényszerítés, vagy más kizsákmányolás áldozatai lesznek.



szerencse2.jpg

Ha valami olyan szépen hangzik, hogy szinte hihetetlen, az nagy valószínűséggel nem is igaz, hanem valamilyen hazugság, átverés. Sajnos sokan még mindig hisznek az ilyen ingyen nyereményekben, és ráadásul meg is osztják a kamu álhíreket.

BOINGBOING / **CORY DOCTOROW** / 6:00 PM FRI FEB 6, 2015

Samsung: watch what you say in front of our TVs, they're sending your words to third parties



Part of the Samsung Smarttv EULA: "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition."

This is part of their speech-recognition tech, which uses third parties (whose privacy policies Samsung doesn't make any representations about) to turn your words into text.

(Image: [fuck tv](#), Jan Ramroth, CC-BY)

[SHARE](#) / [TWEET](#) / **133 COMMENTS**

[GADGETS](#) / [IOT](#) / [T-WEIGHT](#) / [INTERCEPTION](#) / [SURVEILLANCE](#) /

FROM THE BOING BOING SHOP

[See all deals](#)

POPULAR POSTS

George Clooney's neighbor threw a \$27K plate Sanders fundraiser to counter Clooney's \$33K/head Hillary event

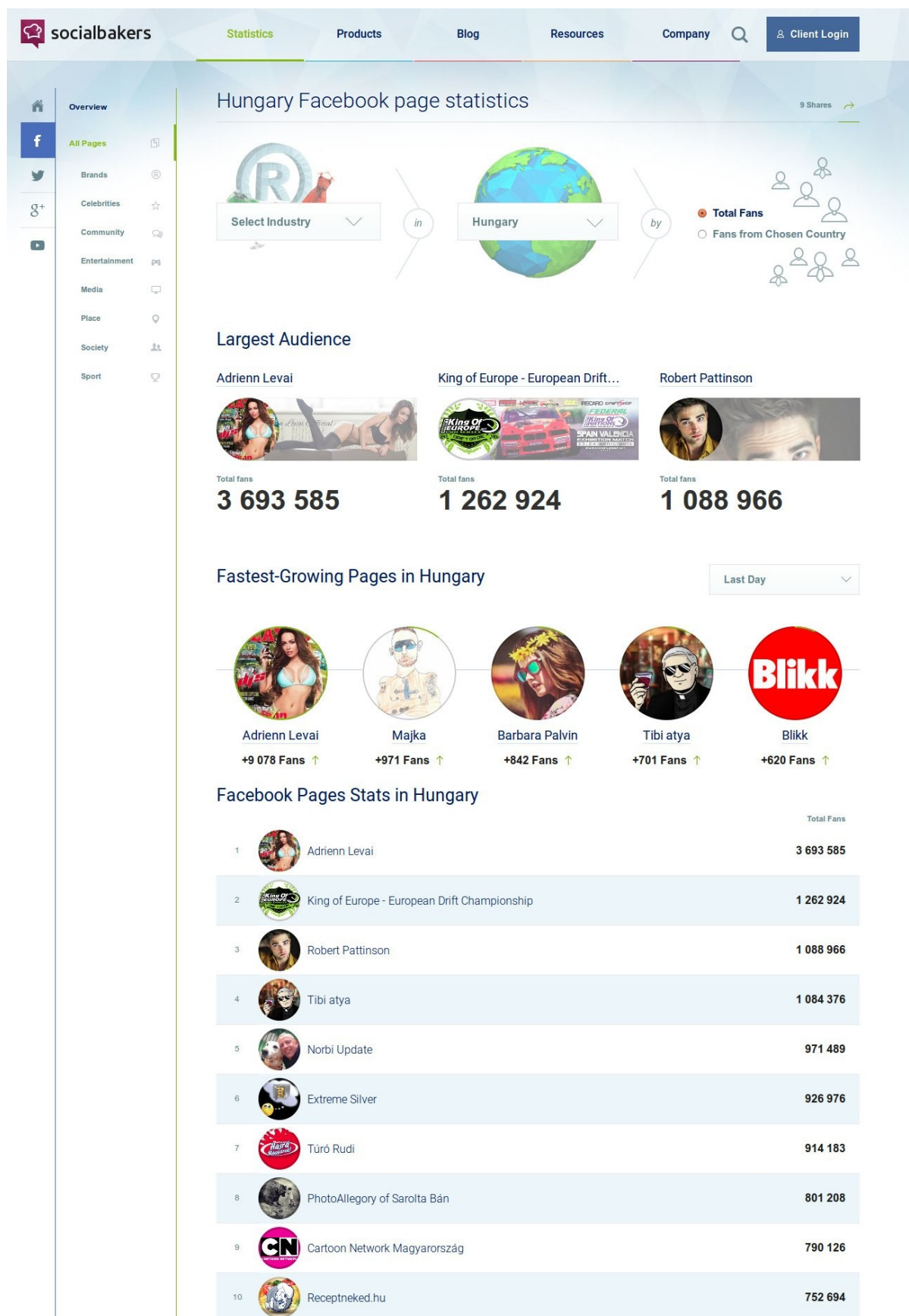
The saga of Ian Bogost's pressure-washer

Barack Obama: Taking money from 1 percenters compromised my politics

Heads of UK's tax havens to Her Majesty's Government: go fuck yourself

samsungtv.jpg

A számtalan internetképes eszköz, köztük az okostelevíziók tartogatnak vaskor meglepetést a felhasználóknak. A többszázoldalas EULA, azaz végfelhasználói szerződésnek sokak által fel sem fedezett része az is, hogy bizalmas beszélgetést lehetőleg ne folytassunk a tévé előtt, mert az rögzítheti, és a hangfelismerés funkció miatt továbbküldheti az interneten.



socialbakers.com_statis.jpg

A Social Bakers magyarországi statisztikájában - amely a Facebook legnépszerűbb tételeit rangsorolja az adott országon belül - nem csak az a meglepő, hogy egy felnőtt filmes hölgy söpri be a legtöbb kedvelést, hanem az is érdekes, hogy egy 2011-es előre lájkolós "mi az indián nevünk" Facebookos átverés elkövetője - egy gyulai ékszerbolt - 5 esztendő elteltével is több, mint 900 ezer FB kedveléssel rendelkezik.



CSALÁDON BELÜLI ERŐSZAK | MODEL | BERENGER ROSE

FELVETTE, AHOGY A MEGVERT FELESÉGE SÍR, HOGY MUTOGASSA A HAVERJAINAK



VELVET

2016.03.09. 10:11

Ajánlom 56

Egy ausztrál modell, Berenger Rose alig két hónap után ment hozzá a barátjához, Shane Cuthberthez. Már korábban kiderült, hogy a férfi agresszív, több rendőrségi ügye is volt. De az elején ez nem jelentett akkora gondot, hamar összeköltöztek, aztán a nő igent mondott. A férje verte, bezárta, ráadásul felvette, ahogy a felesége tele kék-zöld zúzódásokkal könyörög, hogy ne bántsa tovább. Rose most egy [ausztrál tévéműsorban](#) mondta el, mi történt vele. Eddig nem mert nyilatkozni, de a férjét már letartóztatták.

Az interjúban bevallotta, hogy fa rudakkal ütötte, de előfordult, hogy fémre váltott, vagy sajtreszelővel kínoztta.



Minden nap arra gondoltam, hogy én leszek a következő áldozat. Én leszek a következő nő, akit megölnék.



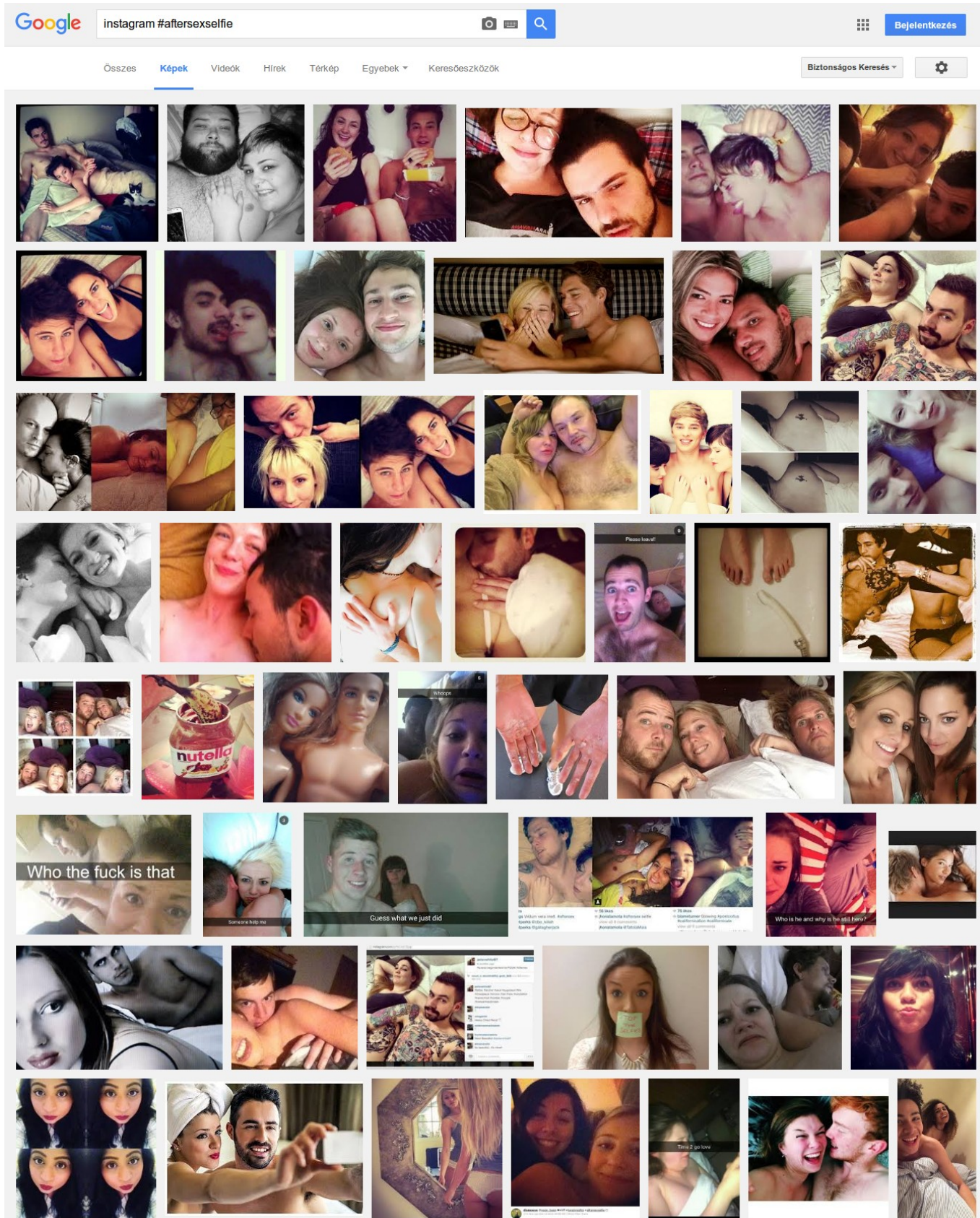
A CURRENT AFFAIR

Fotó: A Current Affair

Cuthberttel az interneten ismerkedtek meg, minden gyorsan történt. Túl sokat nem vártak se az összeköltözéssel, se az esküvővel. Bár a férfi [Instagramján](#) úgy tűnt, hogy imádják egymást, minden oké, nagy szerelem, otthon egészen más zajlott. Shane Cuthbert a kanapén zokogó feleségét videózta, aki azért könyörgött, hogy legyen már vége. A férje meg halálnyugodtan válaszoltatott neki. Mint később kiderült, a barátainak megmutatta a felvételeket, hogy röhögjenek egy jót.

feleseg.jpg

Ahogy a híradóban a hírek is egyre több erőszakról számolnak be, a neten olvasható hírek is bővelkednek szörnyűségekben. Egy ausztrál férfi felesége kínzását és sírását osztotta meg az interneten, hogy barátjaival nevehessenek.



aftersexselfie.png

Eléggé elterjedt az úgynevezett hashtagek között az „#aftersexselfie”, amely közvetlenül a szexuális együttlét utáni fotó megosztását jelenti az interneten. Az intim pillanatokat furcsa módon skalpszerűen közkinccsé tevő divatot sokszor olyan képaláírások kísérik, mint például „ki a fene ez itt az ágyamban?”.

Barbie baba

Engedett a nyomásnak a Barbie babákat gyártó Mattel cég és új modelleket dobott piacra, amelyek nem próbálják uniformizálni a szépséget. Akkor a cég vezetői azt mondták, hogy a babák alakja nem mrceként szolgál, hanem azért alakították így, hogy minél könnyebben lehessen a kiegészítőket és ruhákat cserélni játék közben. Az új modellek bevezetése így valószínűleg leginkább annak köszönhető, hogy 1959-es megjelenése óta a cég eladásai mélyponton vannak és újítaniuk kellett.



barbie.png

A divatlapok címlapjain, TV reklámokban látható csontsovány modellek is hozzájárulhatnak a fiatalok körében tapasztalható egészséges testkép felborulásához. A befolyásolási, manipulálási folyamat már sokszor gyerekkorban elkezdődik, így az abszurd nádszál vékony Barbie babát mostantól igazi, hús-vér átlagos alkatú figurák is követni fogják.

Boston bombing: How internet detectives got it very wrong

By Dave Lee
Technology reporter, BBC News

19 April 2013 | Technology



As the police manhunt stepped up - some members of the public flocked to sites like Reddit to try and find their own clues

Internet users tried for days to piece together clues about the culprits of the Boston bombings. The result? They got it wrong - and left innocent people fearing for their safety. Many are now asking: should "crowd-sourced investigations" be stopped?

Thousands have been tirelessly picking through the evidence - every piece of video footage, every photo, every eyewitness account they can get their hands on.

But this investigation wasn't within the confidential confines of the FBI or local police.

No, these sleuths were working in public - discussing their theories and "leads" within massive communities such as Reddit, 4Chan, Facebook and Twitter.

On Friday, those efforts ended with an apology. After hours of chatter and speculation, the standout suspect identified - and named - was the wrong man.

"I'd like to extend the deepest apologies to the family of Sunil Tripathi for any part we may have had in relaying what has turned out to be faulty information," wrote Reddit user Rather_Confused.

"We cannot begin to know what you're going through and for that we are truly sorry.

"Several users, Twitter users, and other sources had heard him identified as the suspect and believed it to be confirmed.

"We were mistaken."

'Racist Where's Wally'

In the preceding hours, Mr Tripathi, who has been missing since mid-March, became a trending topic on Twitter as his name and picture were shared far and wide.

Information had been gathered on a specially created section on Reddit - known as a subreddit - entitled Find Boston Bombers.

Members had been posting their ideas and footage, offering suggestions over what they saw as crucial clues in what has been described as a crowd-sourced criminal investigation.

Boston bomb trial

When the victims confronted the bomber

How will Dzhokhar Tsarnaev die?

Who is Dzhokhar Tsarnaev?

The 24-page US death penalty form



Wrongly accused Sunil Tripathi, 22, has been missing since mid-March

boston_marathon.png

A közösségi oldalakon terjedő hoaxok, álhírek veszélyesek is lehetnek, hiszen ha valakit igaztalanul vádolnak, vagy rágalmaznak, akkor egy egész felbőszült virtuális tömeg keresheti, meghurcolhatja, bár semmilyen konkrét bizonyíték nem áll a rendelkezésükre. A 2013-as bostoni maratonon történt bombamerényletnél tévesen neveztek meg gyanúsítottként egy ártatlan egyetemi hallgatót, a 22 éves Sunil Tripathi-t.

Hogyan jutnak hozzá a gyerekek?



- **zsebpénzként** kapják
2015 július. 2000 brit szülő megkérdezésével készült felmérés szerint a szülők 25% a digitális pénzben ad zsebpénzt a gyerekeknek (pl. hogy online játékokban, vagy online zene- és videoboltokban elkölthessék)
- **online játékokból** szerzik
- **eladnak** valamit érte (pl. kézműves tárgyakat készítenek, stb.)
- **fejlesztnek** valamit és eladják érte
egyre több gyerek tanul programozni és sokan digitális pénzért cserébe programoznak másoknak
- az Egyesült Királyságban 2014 szeptemberétől érvényes új alaptanterv szerint 5-16 éves korig a közoktatás keretein belül minden évfolyamon kötelező tantárgy a programozás
- **ajándékba** kapják
számos fórumon batorítják a gyerekeket a bitcoin használatára, kisebb összegeket ajándékoznak nekik, ha írnak róla, hogy érdekli őket

btc_zsebpenz.jpg

Egy 2015-ös brit kutatásból az derült ki, hogy az ottani szülők negyede Bitcoinban adja gyermekének a zsebpénzt. Bár ezt okosan is el lehet költeni, sokan nincsenek tisztában azzal, hogy a nehezen lenyomozható virtuális valutáért bármilyen dolgot - fegyvert, drogot, aberrált szexuális szolgáltatást, bérgyilkosságot - is lehet lekövethetetlenül vásárolni a darkweben.

Tízből tíz lány veszélyeztetett, hetet el is adnak prostinak



KOVÁCS BÁLINT | 2016.04.11. 18:19

A naplóm 343

Tweet

G+ 0

A kamaszlány elszökik az intézetből, várja őt a nagyvilág és a pultosmunka Hollandiában – de már a tizenévesek is pontosan tudják, az ilyen utak nem a diszkóba, hanem a bordélyba vezetnek. A gyermekkorukban megerőszkolt, később a gyermekotthonból elcsábított, kurvának eladott lányok története a világ egyik legnagyobb tabutémája. Most mégis két színházi előadás is foglalkozik vele.

„Alexandra vagyok, tizenhét éves. Az egész itt kezdődött tavaly, a nyíregyi pályaudvaron. Egy idősebb barátnőmmel szálltam fel az IC-re, a Kittyvel. Előtte egy szobában laktunk az otthonban, de ő lelépett. Aztán amikor tizenhat voltam, visszajött értem. Azt mondta, segít. Kihúz a retekből. Egy percet nem gondolkodtam. Kiszöktem az otthonból, hogy menjek vele Hollandiába. Azt mondta, a faszija bevisz minket egy ilyen puccos elit diszkóba pultozni. Senkinek nem szóltam, hogy lelépek. Igaz, senki le se szarta.”



Senki nem tud mit tenni (képünk illusztráció)

Forrás: Robin Utrecht/AFP/RU/Robin Utrecht

Ez nem a valóság. Csak színház: így kezdődik a *Kiálllok érted* című előadás, a K.V. Társulat és a Bohócok a Láthatáron közös produkciója Sunnyról és Kittyről, a két nevelőintézetben felnőtt kamasz cigány lányról. Az egyikük már korábban kiment a lehetőségek hazájába, Hollandiába, a másik most követi. Pultozni.

És hiába hallja meg a vonaton egy nála kicsit kevésbé naiv asszony, hiába találkoznak a lányok Kitty korábbi nevelőjével, aki azóta már a minisztériumban dolgozik, senki nem tud mit tenni. Miután az előadás véget ér, tudjuk: Sunny hamarosan munkába áll, de nem lesz sem diszkó, sem pult, csak egy piros lámpa, egy kirakat és egy koszos ágy. És napi néhány tucat férfi.

▼ MOST

10:54 A magyar diadalívet nem rohamozzák a turisták**10:43** Hosszú Katinkát négyen is megelőzték**10:28** Balog Zoltán t faggatják hétfőn a képviselők

eladottlányok.jpg

Sajnos már Magyarországon is reális veszély a fiatal lányok behálózása, és a hamis ígéretek, vagy éppen az elrablásuk után rémisztő helyzetben találhatják magukat: adják-veszik őket prostituáltként.

Házibulin erőszakolták meg a 15 éves lányt

INDEX

2016.03.10. 10:10

Ajánlom 3

Gyermekpornográfia büntette miatt négy ember ellen emelt vádat a Budapesti I. és XII. Kerületi Ügyészség – tájékoztatta a **Magyar Nemzetet** a Fővárosi Főügyészség.

2013-ban egy XVII. kerületi házibuliban vettek részt, és felvételt készítettek arról, hogy két társuk közösen egy ittas 15 éves lánnyal. A fiatalok a videót e-mailben több ismerősüknek is elküldték. A vádlottak közül hárman még maguk is fiatalkorúak, azaz 18 éven aluliak voltak.

Ugyanebben az ügyben eredetileg kiskorú sértett sérelmére, szexuális erőszak miatt is indult nyomozás a szexuális aktusban részt vevő 18 éves budapesti fiatal és egy 19 éves olasz állampolgár ellen. Ezt az eljárást időközben megszüntették, mert a hatóság a tanúvallomások alapján nem látta kétséget kizáróan bizonyítottak, hogy a lány akaratnyilvánításra képtelen állapotban lett volna. Noha a nyomozást megszüntető határozat ellen panaszt jelentettek be, de azt a Fővárosi Főügyészség végül elutasította.

A büntető törvénykönyv szerint az, aki tizennyolcadik életévét be nem töltött személyről vagy személyekről pornográf felvételt szerez meg vagy tart, három évig terjedő szabadságvesztéssel büntethető. Aki viszont ilyen felvételt készít, kínál, átad vagy hozzáférhetővé tesz, egytől öt évig terjedő szabadságvesztést kaphat - írja a Magyar Nemzet.

eroszak_video.jpg

Az okostelefon kamerájával készítettek felvételt egy leitatott 15 éves lány megerőszakolásáról, majd a felvételt ismerőseiknek továbbküldték - az ilyen bűncselekményekből sajnos már hazai esetek is előfordulnak.

TECH

7,500 Online Shoppers Unknowingly Sold Their Souls

Published April 15, 2010 · FoxNews.com



A computer game retailer revealed that it legally owns the souls of thousands of online shoppers, thanks to a clause in the terms and conditions agreed to by online shoppers.

The retailer, British firm [GameStation](#), added the "immortal soul clause" to the contract signed before making any online purchases earlier this month. It states that customers grant the company the right to claim their soul.

"By placing an order via this Web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant Us a non transferable option to claim, for now and for ever more, your immortal soul. Should We wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it, within 5 (five) working days of receiving written notification from gamesation.co.uk or one of its duly authorised minions."

[GameStation's form](#) also points out that "we reserve the right to serve such notice in 6 (six) foot high letters of fire, however we can accept no liability for any loss or damage caused by such an act. If you a) do not believe you have an immortal soul, b) have already given it to another party, or c) do not wish to grant Us such a license, please click the link below to nullify this sub-clause and proceed with your transaction."

The terms of service were updated on April Fool's Day as a gag, but the retailer did so to make a very real point: No one reads the online terms and conditions of shopping, and companies are free to insert whatever language they want into the documents.

While all shoppers during the test were given a simple tick box option to opt out, very few did this, which would have also rewarded them with a £5 voucher, [according to news:lite](#). Due to the number of people who ticked the box, GameStation claims believes as many as 88 percent of people do not read the terms and conditions of a Web site before they make a purchase.

Trending in Tech

- 1 5 password mistakes you can't afford to make
- 2 Electric rain? Solar panel turns raindrops into power
- 3 DARPA's new Gremlin drones fly back to their 'motherhip' after completing recon missions
- 4 Apple wants judge to reject DOJ appeal in Brooklyn drug case
- 5 'Dark Souls 3' review: Difficult but totally rewarding

See all Trends

SCITECH CONNECT

Subscribe to the daily Geek Sheet for the top science and technology stories.

you@domain.com

SUBSCRIBE →

f Tetszik

65 ez

Follow @fxnscitech

eula_soul.jpg

Egy klasszikus példa arra, hogy milyen veszélyeket rejt az, ha valaki nem olvassa el a felhasználói licencszerződést. A kicsit vicces kísérletben próbaképpen azt is beírták az EULA-ba, hogy aki elfogadja, az eladta a lelkét. Ami viszont már egyáltalán nem vicces, hogy általában sokan nincsenek tisztában, hogy pontosan miket is fogadtak el valójában egy next-next-finish telepítés során.

Az FBI üzemeltetett egy gyerekpornó-oldalt

INDEX

2016.01.23. 10:15

 Ajánlom

32



Az FBI átvette és üzemeltette az internet egyik legnagyobb gyerekpornó-oldalát, hogy elkapjon több ezer pedofilt. Az **egyikük most perli a kormányt**, amiért az ügynökség hozzáférést engedett neki a honlaphoz.

Az amerikai igazságügyi minisztérium bírósági iratokban elismerte, hogy az FBI üzemeltette a Playpen nevű oldalt egy titkos művelet keretében. 2015. február 20-tól, ahelyett, hogy lekapcsolták volna a lefoglalt weboldalt, az FBI egészen május negyedikéig működtette, és megfertőzte a látogatókat olyan kóddal, ami felfedte valós identitásukat. A gyerekpornós weboldalak az úgynevezett sötét weben futnak, ez a Tor nevű proxyhálózatból érhető csak el, egyszerű böngészőknek és a keresőknek láthatatlan.

A weboldalnak több mint 215 ezer regisztrált felhasználója volt, több mint 23 ezer szexuálisan explicit fotója és videója gyerekekről, közülük 9000 ezret közvetlenül az FBI szervereiről lehetett letölteni, Washingtonból.

A hatóságok 1300 felhasználó számítógépéhez fértek hozzá és azonosították be őket, közülük 137 ellen sikerült vádat emelni. Az egyikük, egy középiskolás szerint viszont az FBI tehet az egészből: "amit a kormány tett ebben az esetben, olyan, mintha elárasztanám a környéket heroinnal, hátha elkapok valakit droghasználatért" – érvel. Ügyvédje azt kéri, ejtsék ellene a gyerekpornós vádakat.

Korábban nem ez volt az FBI stratégiája, ha lefoglaltak egy oldalt, egyből le is kapcsolták, mivel a bírói döntések alapján, "minden alkalommal, amikor valaki megnéz egy gyerekpornográf-felvételt, a gyerek sérül". Most viszont azt nyilatkozta az FBI, hogy "volt egy lehetőségünk, és semmi nem szólt ellene. Az USA Today szerint ez volt az első ilyen típusú akció.

fbi_honeypot.jpg

Az FBI minden lehetséges eszközzel igyekszik a pedofil elkövetők lekapcsolására, így például 2015-ben egy titkos művelet keretében csali oldalt működtettek és megfigyelték a gyermekpornó után érdeklődött felhasználókat.

MÉG CSAK 17 ÉVES, DE A HÉT MINDEN NAPJÁRA VAN LUXUSAUTÓJA



KAVICS

KÖVETÉS

2016.04.15. 14:48

Ajánlom

Az [Insta gazdag kőlykei sorozatunk](#) legújabb szereplője a 17 éves Jack Watkins, aki elődeihez méltó módon előszeretettel kérkedik anyagi javaival az interneten. Életéről sokat elmond, hogy csak februárban szerezte meg a jogosítványt, mégis 660 millió forint értékben vannak luxusverdái. Hogy honnan volt pénze ilyesmire? Hát persze, hogy a szüleitől!



Fotó: youtube

A [Sun szerint](#) az ifjú titán és családja Cheshire városában él, ahol kitartó pénzszerőrással érték el, hogy kevésbé szerencsés polgártársaik a brit Kardashianék néven emlegessék őket. Mielőtt még elmerülnék a részletekben, vegyünk szépen sorra, milyen kocsik parkolnak Jack Watkins garázsában:

- egy Rolls-Royce
- két Bentley
- két Mercedes-Benz
- egy Range Rover Vogue
- és egy Porsche

Tehát, lényegében a hét minden napjára van egy nagyon drága autója.

Jack Watkins csodálatos élete persze nem csak a menő kocsikkal való kérkedésből áll. Szívesen eldicsekszik azzal is, hogy szülei magánrepülőjével utazik egzotikus helyekre, hogy aztán csillagászati összegeket verjen el mindenféle dizájner holmira. A srác elég komolyan veszi a dolgot, egyszer például 500 ezer fontot, mintegy 195 millió forintot adott ki egy Bvlgari órára.



Fotó: youtube

"Már megszoktam, hogy az emberek féltékenyek rám - legyenek akár felnőttek vagy tinédzserek"

– mondja Jack Watkins, aki olyan szempontól is szerencsésnek tartja magát, hogy remekül képes kezelni az irigykedőket.

gazdagsag_instagram.jpg

Sokan igyekeznek szebbnek, okosabbnak, szerencsésebbnek vagy gazdagabbnak feltüntetni magukat a közösségi oldalakon. Van viszont egy olyan kör is, akik elképesztő gazdagságukat fitogtatják képekkel: magánrepülővel járnak iskolába, Roll Royce motorháztetőről eszik a kaviárt, vagy mindennap másik sportkocsival pózolnak.

A kérdés



Lehet megis terhes a barátnőm? December 10. en pettingeltünk es lehet elovaladekos volt a kezem amikor megujaztam december 16. an megjött neki.23. -an csinalt egy tesztet es negativ.

🕒 ma 15:14

✉ [Privát üzenet](#)

👍 [Tetszik](#)

A válasz



nem.

1/1

🕒 ma 15:20

✉ [Privát üzenet](#)

Hasznos számodra ez a válasz?



☐ Értesítsünk róla, ha új válasz érkezik?

Válasz küldése

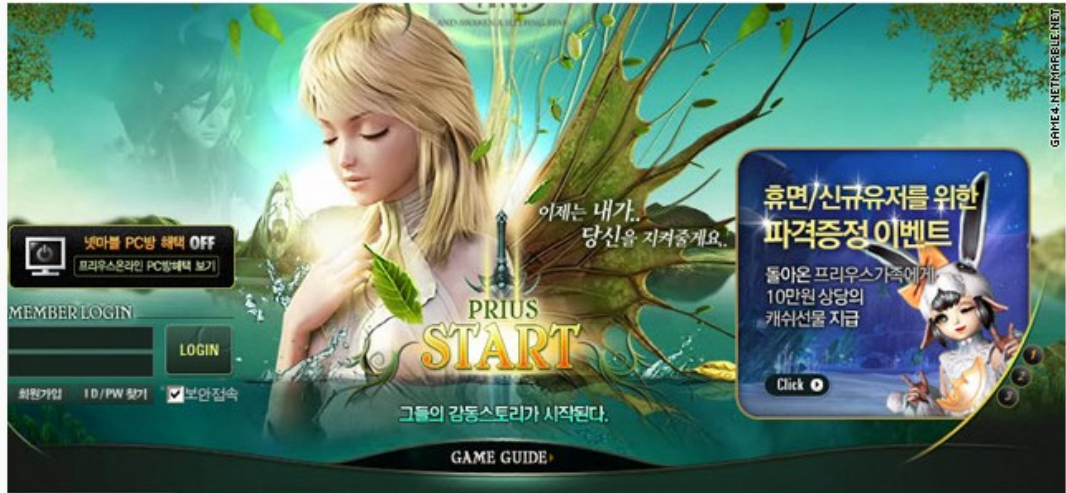
gyakori_kerdesek.png

Egy tipikus példa arra, hogy ha nem tőlünk kérdez a gyerek, az nem azt jelenti, hogy nincsenek neki kérdései, hanem ezeket valószínűleg másoknak fogja feltenni.

Jail for couple whose baby died while they raised online child

By **Andrew Salmon**, For CNN

May 28, 2010 -- Updated 1146 GMT (1946 HKT)



STORY HIGHLIGHTS

- Couple's baby starved to death while they raised a virtual child
- Court hands out two-year sentence; mother's suspended
- Couple is expecting another child in August
- Internet gaming popular in South Korea, home to 21,500 Internet cafes

RELATED TOPICS

[South Korea](#)
[Internet](#)

Seoul, South Korea (CNN) -- A couple whose baby starved to death while they raised a virtual child in an online fantasy game was sentenced Friday, their defense attorney said.

Prosecutors at Suwon District Court had sought a five-year sentence for negligent homicide, but the court handed out a two-year sentence.

Sentence was suspended for the female defendant, Kim Yun-jeong, 25, who is expecting the couple's daughter in August. Her partner, Kim Jae-beom, 41, will serve two years.

The unmarried couple's defense attorney said he was satisfied with the sentence.

"This is the first legal case regarding Internet addiction in Korea," said Kim Dong-young, a lawyer with the Korean Legal Aid Corp. "I am pleased that the female defendant's Internet addiction was taken into consideration, and she was bailed."

Three-month-old Kim Sa-rang died of malnutrition in September while her parents were engaged in 12-hour sessions of Prius Online. In the 3-D fantasy game, players nurture an online girl who gains magical powers as she grows.

Kim's mother is a former factory worker while her father is a taxi and truck driver.

During their trial, the court heard that the toddler weighed 6.4 pounds (2.9 kgs) when she was born, but was only 5.5 pounds (2.5 kgs) at the time of her death.

gyerekhalal.png

Sajnos elképesztő és szomorú esetek is megtörténnek időnként, 2010-ben egy dél-koreai házaspárnak elhanyagolás miatt éhen halt a gyermeke - a kicsi holtteste mindössze 2.9 kg volt - amíg a szülők rá voltak kattánva az állandó online játéokra.

SZINTE NINCΣ KORHATÁR A GYERMEKPROSTITÚCIÓBAN



UT

+ KÖVETÉS

2013.08.02. 10:27

f Ajánlom

3,3 ezer



A neve és arca elhallgatását kérő, biztonsági okok miatt részletesen a munkamódszereiről sem beszélő gyermekvédelmi szakember több mint tíz éve harcol a gyermekprostitúció ellen, ha kell, félhivatalos módszerekkel. Nevelőként dolgozik, emellett eltűnt intézetis vagy szegénytelepeken élő gyerekek után kutat, az elmúlt években csaknem kétszázat hozott haza, többségüket külföldről, ahol prostituáltként kerültek elő. Mivel a probléma magján, azaz a prostitúció iránti keresleten változtatni képtelenség, úgy véli, a gyermekvédelmi rendszert kellene megreformálni. Különleges helyzetét és akcióit tekintve saját kérésére nem hozhatjuk nyilvánosságra sem az ő, sem az őt alkalmazó intézetek és alapítványok nevét.

Hány fiatakorúért mentél külföldre?

Kétszáz esetben hoztam vissza lányokat és elenyésző számban fiúkat is, nagy részüket prostituáltként dolgoztatták. Hollandiát, Németországot és Ausztriát egyaránt járom.

Mindez gyermekvédelmi szakemberként benne van a munkakörödben?

Ezek partizánakciók. Privát emberként megvannak a szükséges kapcsolataim, Magyarországon kívül több ország rendőrségével is.

Hány éves volt a legfiatalabb lány, akit hazahoztál?

A legfiatalabb egy tizenkét éves heroinfüggő, hepatitiszes lány volt Hollandiából. Intim herpesz volt a száján és a kezén. Sajnos szinte nincs alsó korhatár. Egyszer elkaptam Bécsben vagy Berlinben egy lányt, és húsz percen belül hívtak az egyik kisvárosi rendőrségtől, hogy a család háza előtt a stríci kijelentette, ha nem lesz meg a gyerek, viszi a kisebbet. A tíz-tizenkét éves lányok is veszélyben vannak. Mindig azt mondom, Európa Thaiföldje vagyunk – tényleg így gondolom, bár ott van még az elég nagy Balkán is a maga szegénységével. A szegénység pedig egyszerre vonzza és szüli mindezt.

gyermekvedelmis.jpg

Kőkemény valóság egy elhivatott gyermekvédelmi szemével, aki a külföldre hurcolt, kábítószerfüggő és prostitúcióra kényszerített gyereklányoknak próbál meg segíteni, olykor a legalitás határát súroló kalandos eszközökkel menekíti haza az áldozatokat.

283256.

2012.06.08. 10:42

★★★★

válasz

Van bárki, aki HOLNAP /06.09. SZOMBAT/ bármikor, Budapesten a Blaha Lujza tér közelében el tudna adni számomra -személyes átvétellel- 1 doboz 100 db-os 2 mg-os Rivotrilrt???

283202.

2012.06.07. 19:25

★★★★

válasz

Korlátozott darab számban FRONTIN 1mg/90 Eladó



283094.

2012.06.06. 20:42

★★★★

válasz

Egy bontatlan Rivotril 2mg 100x. 4000-2016.-lg jó a szavatossága.

Budapesten vehető át. Átvétel előtt természetesen megtekinthető. Házhoz szállítás is megoldható futárszolgálattal, Budapest területén.

POSTA ÉS TELEFON KIZÁRVA!

Érdeklődni lehet:

Cikk betűmérete: - +

303561.

2015.10.30. 12:45

★★★★

előzmény

válasz

Engem érdekelne a Frontin.

303542.

2015.10.29. 11:02

★★★★

előzmény

válasz

A Contramal 200 mg-os érdekelne, de csak eredeti levélben vagy csomagolásban. A részletekről vagy a tel. számamon. vagy az email címemre írj kérlek. Sürgős lenne.

303533.

2015.10.28. 10:30

★★★★

válasz

ez lemaradt

303532.

2015.10.28. 10:29

elft0r

★★★★

válasz

Contramal 200mg Frontin 1mg Xanax 1mg és 05 is Rivo 2 doboz 2es 100as Rilex 2.5 posta kizárt csak Budapest személyesen

KERESŐ (0 TALÁLAT) "TENISZLABDA"

Gyakori keresések: rivotril kompresszor | fűrógép | bmw | ingyen | ingyen elvihető | Dorog | csere | hegeszto | volvo | kony | polc | erosito | mercedes | tyuk | hentes | simson | monitor | fűnyíró | eger | hifi | switch | mosógép | miskolc | hitel | sofőr | televízió | hostess | pécs | cnc |

gyogyszerek_1.jpg

A gyakori keresőtálatatok között szerepelnek a különféle gyógyszerek is, amelyekhez könnyen hozzá lehet jutni. Sokan nem csak rendszeresen szednek ilyeneket, hanem alkohollal együtt fogyasztják ezeket.



29 ATM Skimmer Gang Firebombed Antivirus Firm

SEP 15



It's notable whenever cybercrime spills over into real-world, physical attacks. This is the story of a Russian security firm whose operations were pelted with Molotov cocktail attacks after exposing an organized crime gang that developed and sold malicious software to steal cash from ATMs.

The threats began not long after December 18, 2013, when Russian antivirus firm **Dr.Web** posted a writeup about a new Trojan horse program designed to steal card data from infected ATMs. Dr.Web received an email warning the company to delete all references to the ATM malware from its site.



The anonymous party, which self-identified as the "International Carders Syndicate," said Dr.Web's **ATM Shield** product designed to guard cash machines from known malware "threatens activity of Syndicate with multi-million dollar profit."

The threat continued:

"Hundreds of criminal organizations throughout the world can lose their earnings. You have a WEEK to delete all references about ATM Skimmer from your web resource. Otherwise syndicate will stop cash-out transactions and send criminal for your programmers' heads. The end of Doctor Web will be tragic."

In an interview with KrebsOnSecurity, Dr.Web CEO **Boris Sharov** said the company did not comply with the demands. On March 9, 2014, someone threw a Molotov cocktail at the office of a third-party company that was distributing Dr.Web's ATM Shield product. Shortly after that, someone attacked the same office again. Each time, the damage was minimal, but it rattled company employees nonetheless.

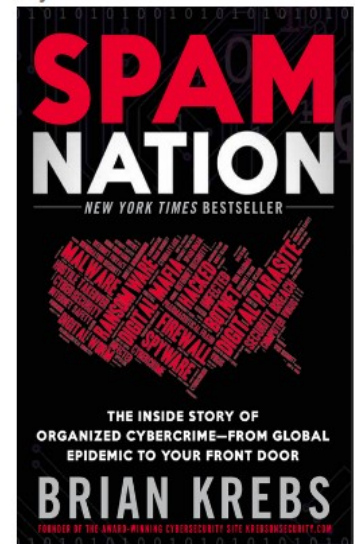
Less than two weeks later, Dr.Web received a follow-up warning letter:

"Dear Dr.Web, the International carder syndicate has warned you about avoidance of interference (unacceptable interference) in the ATM sphere. Taking into account the fact that you've ignored syndicate's demands, we employed sanctions. To emphasis the syndicate's purpose your office at Blagodatnaya st. was burnt twice.

If you don't delete all references about atmskimmer viruses from your products and all products for ATM, the International carder syndicate will destroy Doctor Web's offices throughout the world. In addition, syndicate will lobby the Prohibition of usage of Russian anti-viruses Law in countries that have representation offices of the syndicate under the pretext of protection against Russian intelligence service."

After a third attack on the St. Petersburg office, a suspect who was seen running away from the scene of the attack was arrested but later released because no witnesses came forward to confirm he was the one who threw the bomb.

My New Book!



A New York Times Bestseller!

[Buy at Amazon](#)

Recent Posts

[Security Bug in Dell PCs Shipped Since 8/15](#)
[How to Enable Multifactor Security on Amazon](#)
[ISIS Jihadi Helpdesk Customer Log, Nov. 20](#)
[Starwood Hotels Warns of Credit Card Breach](#)
[Federal Legislation Targets "Swatting" Hoaxes](#)

Subscribe by email

Please use your primary mailbox address, not a forwarded address.

Your email:

[Subscribe](#)

[Unsubscribe](#)

Support KrebsOnSecurity!

[Donate](#)



gyujtobomba.png

Amikor az internetes leleplezés fizikai erőszakba torkollik. Miután az ATM pénzautomatákat megfertőző bűnözők viselt dolgairól beszámoltak a Dr. Web antivírus cég szakemberei, moszkvai irodájukra ismeretlenek gyújtóbombát dobtak.

Úgy érzik, csak halállal szabadulhatnak az iskolától



SZABÓ DÁNIEL VILMOS

2016.04.11. 21:17

Ajánlom

132



Az interneten otthon is folytatódik az iskolai bántalmazás és a kiközösítés. Az áldozatok a legtöbbször elhiszik, hogy bennük van a hiba, sokan nem bírva a terhet az öngyilkosságot választják. Pedig a zaklatás kezelhető, és kívülről is felismerhető, ha valakit bántanak. A segítség is közelebb van, mint a gyerekek gondolnák.

”Nincs más módja annak, hogy elkerüljem az iskolát (...) Apa, arra tanítottál, hogy jó ember legyek és tartsam be az ígéreteimet... Mama, nagyon jól gondoskodtál rólam és sok helyet mutattál meg!

– írta a búcsúlevelében Diego, egy tizenéves spanyol kisfiú, aki tavaly októberben lett öngyilkos az öt évtől iskolai zaklatás miatt. Hiába kérte, hogy hadd maradjon ki, néhány alkalmat eltekintve, mindig be kellett mennie az iskolába. Nem tudni, hogy pontosan mivel zaklatták a társai, de egyszer több hétre elment a hangja, miután torkon vágta, írja az *El Mundo*.

Diego nem beszélt a vele történetéről, és utólag sem derült ki semmi a bántalmazásokról, a hatóságok lezárták az ügyet. A szülők azért hozták nyilvánosságra fiúk levelét, hogy az iskolában végre rend legyen, és más gyerek ne kerüljön reménytelen helyzetbe a zaklatói miatt.

Már nincs menekvés

Az internet elterjedésével a bántalmazott diákok otthon is utolérik a zaklatói. Emiatt a szakemberek ezt tartják a modern oktatás egyik legnagyobb problémájának.

”Minden nap beszóltak, hogy egy »dagadt kocka« vagyok. Aztán megvették a játékot, ahova elmenekültem előlük, a virtuális terembe. De még a havidíjat is kifizették azért, hogy az internetes szerepjátékban zaklathassanak

– ezt a történetet már egy 14 éves fiú mesélte nekem a saját élményeiről. Ő két éve kísérelt meg öngyilkosságot, de végül maga hívta ki a mentőket. Csak azért kezdték el piszkálni a társai, mert

halal_zaklatas.jpg

Az internet zaklatás minden országban, így nálunk is jelentős probléma. A zaklatás, az internetes bántalmazás akkor sem szünetel, ha véget ér a tanítás, hanem a virtuális térben gyakran még otthon is folytatódik.

Így vert át 2015-ben az internet

2015.12.31. 06:49, Kívül tágasabb , 3 komment

Még mindig nem tanultuk meg, hogy az interneten feltűnő sztorik, képek, videók egy részét nem árt fenntartásokkal kezelni, és itt nem csak a csodatévő, rákot elmulasztó, titkos gyógymódokról, vagy az egészen elképesztő összeesküvés-elméletekről van szó, hanem a mindennapi hírek kapcsán előkerülő képekről is.



Nem meglepő, hogy 2015-ben is sok hamis fotó és videó száguldott végig az interneten, ezek egy része ráadásul nem feltétlenül véletlenül, akadtak, melyeket kifejezetten az olvasók félrevezetése érdekében hamisították meg. Lássunk ezek közül pár példát [a BBC gyűjtésének segítségével!](#)

A nepáli földrengés legmeghatóbb képe

Áprilisban történt az év egyik legnagyobb természeti katasztrófája, a nepáli földrengés, melyben 7652-en veszítették életüket, több mint 16 ezren megsérültek, és közel 200 000 lakóház megsemmisült.

A kép, melyen egy négyéves kislány védelmezően karolja át két éves kishúgát bejárta a világot, a Facebookon és a Twitteren is rengetegen megosztották, adakozásra szólítva fel az embereket.

internetes_atveres.png

A manipuláció gyakran előkerül, ha valamilyen tragédia történik. Az állítólagos jótevékenységek, illegális adománygyűjtők az átlagemberek részvételét igyekeznek kihasználni, és ehhez hamis fotókat is felhasználnak.

NEWS

[Home](#) | [Video](#) | [World](#) | [UK](#) | [Business](#) | [Tech](#) | [Science](#) | [Magazine](#) | [Entertainment & Arts](#)[World](#) | [Africa](#) | [Asia](#) | [Australia](#) | [Europe](#) | [Latin America](#) | [Middle East](#) | [US & Canada](#)

Sydney schoolgirl 'wired cash to IS'

🕒 3 hours ago | [Australia](#)

A teenage girl and a 20-year-old man will face court in Sydney accused of sending money to the so-called Islamic State from Australia

A Sydney girl, 16, has appeared in court on terror financing charges which carry a maximum term of 25 years' jail.

She is accused of sending thousands of dollars to the so-called Islamic State group in Syria through a Western Union money transfer, reports say.

The girl and a male accomplice, 20, who allegedly gave her the money were arrested in raids on Tuesday.

The pair allegedly met in a park on Tuesday to discuss a plan to send money to Syria that day, reports said.

They had reportedly developed a "sophisticated facilitation path" of wiring funds and had completed successful transfers before.

The man, named by media as Milad Atai, was also arrested during Australia's biggest counter-terror raids in September 2014.

Transfers

The girl is accused of admitting to a police informant that she had wired A\$10,000 (\$7,600, £5,400) to Syria at the behest of an Islamic State fighter.

She was also allegedly planning to conduct another transfer of A\$5,000 when she was caught on Tuesday morning in a park along with Mr Atai, who had handed her the money.

isis_atutalas.jpg

Abból is baj lehet, ha valaki csak a neten tudatlanul, naivan tesz olyat, amit nem kellene. Egy ausztrál középiskolás lány 25 évnyi börtönbüntetéssel néz szembe, mert szíriai barátja kérésére pénzt utalt át az Iszlám Állam számlájára.

AKTUÁLIS » Belföld » Szexvideóval állt bosszút a megcsalt középiskolás

Szexvideóval állt bosszút a megcsalt középiskolás

ma 04:00

FÉLTÉKENYSÉG BOSSZÚ KAMASZOK SZEKVIDEÓ



A fiú feltöltötte a Facebookra a videót, amelyen 15 éves barátnőjével szexelt

Koós Szabolcs
főmunkatárs

Szexvideóval állt bosszút egy kamasz fiú, miután megcsalta őt barátnője. Az ügyben rendőrségi nyomozás is indult, a történet ugyanis jóval komolyabb egy tinicsetepaténál.

A tinik videóra vették az aktust

Tihamér és Rózsa (a fiatalok névének védelme érdekében a szereplők nevét megváltoztattuk – a szerk.) a nógrádi megyeszékhely egyik középiskolájában tanulnak, a két 15 éves diák nem is olyan régen még egy párt alkotott.

És bizony nemcsak moziba jártak, és lépcsőházban csókolóztak: a gyerekek már a szexben is járatosak voltak, mi több, **videóra rögzítették az aktust**. Talán soha nem is derült volna ki a dolog, ha a szerelmes kamasz fiú nem tudja meg, hogy **kedvese az egyik iskola tanárával is bensőséges viszonyba került**.

– A tanár, akiről szó van, bőven az apja lehetne Rózsának. Amikor Tihamér megtudta valakitől a dolgot, **dühében feltöltötte a videót** a Facebookra. Az egész iskola végignézte, lájkolta, Rózsa pedig majd elsüllyedt szégyenében – mesélte a Blikknek a fiatalok egyik ismerőse, hozzátéve: úgy tudja, az ügyben a lány szülei feljelentést tettek.

Mivel nem tudták, hogy milyen törvényt sértett a hiú fiatalember az aljas bosszúval, ezért mindent elmondtak a rendőrségen, s a hatóságra bízta, hogy eldöntsék, történt-e törvénytörés, indítanak-e eljárást.

iskolai_szexvideo.jpg

Magyar középiskolai diákok között is sokan videóra veszik a szeretkezésüket párjukkal. Abba viszont sokan nem gondolnak bele, mi lesz, ha mindez illetéktelen kezekbe kerül, illetve ha a szakítás után a másik fél bosszúból feltölti, megosztja.

Egy 2014-es felmérés szerint a 9-18 éves kamaszok 67%-a találkozott már az interneten pornográf tartalommal és ebből csak 10% volt az, aki kifejezetten ilyen céllal kapcsolta be a számítógépet.

A megkérdezett fiatalok 8 %-ának az élmény kifejezetten kellemetlen, zavaró volt.

kamaszok.png

Egy felmérés szerint a kamaszok 67% találkozott már pornográf tartalommal az interneten. Az adat kissé hihetetlen, a 100% talán közelebb lehet a valósághoz.

KATEGÓRIÁK

- [Főoldal](#)
- [Tini párkapcsolatok](#)
- [Szerilem](#)
- [Randizás](#)
- [Társkeresési problémák](#)
- [Párvkapcsolatok](#)
- [Egyéb kérdések](#)
- [Új kérdés](#)
- [Kategoría toplista](#)

NÉPSZERŰ TÉMÁK

- Barát Barátnő
- Barátság
- Beszélgetés
- Buli
- Csaj Csók Esély Ex
- Facebook
- Fiatal
- Flú
- Iskola
- Ismerkedés
- Kapcsolat
- Karácsony
- Lány
- Osztálytárs
- Pár
- Párvkapcsolat
- Pasi
- Probléma
- Randi
- Srác
- Szakítás
- Szerilem
- Szeretet
- Szex
- Tetszik
- Tini



Tini párvkapcsolatok - Gyakori kérdések

Kérdések	Új kérdés	Kiemelt kérdések	Válasz nélküli kérdések	Kulcsszavak
?	Még volna esélyem, hogy visszaszerezem?	1 válasz		
Kategória:	Szerilem			
?	Mit tegyek szerintetek? Kezdeményezzek vagy sem?	5 válasz		
Kategória:	Szerilem			
?	Hogyan tudnám legyőzni a lefagyásom?	7 válasz		
Kategória:	Szerilem			
További kiemelt kérdések (összesen 22) »				
Friss	Baj, hogy nekem a 19 év feletti fiúk tetszenek inkább?	4 válasz		
Kategória:	Egyéb kérdések			
Friss	Szerintetek mit csináljak? Pár hónapja lekoptatott ez a csaj mostmeg teper nálam!	1 válasz		
Kategória:	Szerilem			
Friss	Vajon érdekel engem?	1 válasz		
Kategória:	Szerilem			
Friss	Ez jogos volt? Szerintetek melyikünk a hibás?	4 válasz		
Kategória:	Párvkapcsolatok			
Friss	Azt kérdeztem egy lánytól hogy nem -e akarunk barátok lenni. Most hogyan tovább?	3 válasz		
Kategória:	Párvkapcsolatok			
Friss	Hogy tudnék ezen javítani?	1 válasz		
Kategória:	Egyéb kérdések			
Friss	Szerintetek járunk? (Többi lent)	4 válasz		
Kategória:	Szerilem			
Friss	Barátomnak nincs ideje rám, nem foglalkozik velem. Miért? Mit tegyek?	1 válasz		
Kategória:	Párvkapcsolatok			
Friss	Szerintetek, ha egy lánynak szerelmet vallottam de ő nem érez irántam semmit akkor még lehetünk barátok?	3 válasz		
Kategória:	Szerilem			
Friss	Ezzel szerintetek célozni akart rá?	2 válasz		
Kategória:	Egyéb kérdések			
Friss	13-16 évesen mit csináltok egy kapcsolatban?	3 válasz		
Kategória:	Párvkapcsolatok			
Friss	Cikl a három év korkülömbőség?	8 válasz		
Kategória:	Szerilem			
Friss	Mit tegyek mi lenne a helye? Mit tegyek ha elmegy nélkülem? Szeret igazán ezek alapján vagy?	1 válasz		
Kategória:	Szerilem			
Friss	Nemtudok leállni de van szexet meg nem akarom mitcsináljak?	4 válasz		
Kategória:	Egyéb kérdések			

kerdes_az_van.png

Az egyik legjobb tanács, hogy legyünk jóban és rendszeresen beszélgetssünk a gyerekünkkel gondjairól, virtuális életéről. Ahogy korábban is említettük, ha minket nem kérdez, akkor biztosak lehetünk benne, hogy máshol keresi a válaszokat, mert kérdések azok mindig vannak.

MAGYARORSZÁGRA JÁRT MEZTELEN KISLÁNYOKAT FOTÓZNI



VIK

+ KÖVETÉS

2016.02.23. 16:54

Ajánlom 0

10-10 ezer forintot fizetett egy férfi még 2013-ban két kislánynak azért, hogy levetkőzzenek előtte, és hagyják magukat lefényképezni. A külföldi férfi tárgyalása február 23-án, kedden kezdődött a Nagykanizsai Járásbíróságon.

Mivel a kislányoknak pénzre volt szükségük, a férfi könnyedén a kegyeikbe férkőzött: először édességekkel, ruhákkal, cipőkkel és egyéb ajándékokkal halmozta el a gyerekeket, akik végül belementek a fotózásba. A lányokról összesen 73 fénykép készült.

A rendőrség a házkutatás alatt számtalan fotót és pornográf videót talált, amelyeken – a szakértők szerint – kilencvenen biztosan 18 év alattiak voltak.

A férfi, amikor épp Magyarországon volt, általában áthívta magához a lányokat, de egy idő után már maguktól is mentek, ha éppen pénzre volt szükségük.

Kedden a bíróság csak a vádlottat hallgatta meg, végül a tárgyalást elnapolták.

kulfoldi.jpg

Olyan eset is előfordul, hogy külföldiek pénzzel, ajándékokkal kenyerезnek le fiatakorúakat, és készítenek róluk meztelen fotókat, videókat. A hirtelen, megmagyarázhatatlan pénzkereset, váratlan drága ajándékok felbukkanása a gyerekeknél figyelmeztető jel lehet a szülőknek.

High school teen hailed as a hero after defending a blind classmate who was being beaten by a bully

- Teen was hailed as a hero for **defending a blind classmate who was being beaten up**
- Huntington Beach High School student **floored bully with a single punch**
- **Unnamed bully was today arrested on suspicion of misdemeanor battery**

By HANNAH PARRY FOR DAILYMAIL.COM

PUBLISHED: 02:48 GMT, 25 September 2015 | UPDATED: 14:22 GMT, 27 September 2015

Share 50k shares 1.3k View comments

A California teenager has been hailed as a hero after he rushed to help a blind classmate being beaten up by a bully.

Shocking footage of the attack, filmed by a bystander, shows the 'visually impaired' student being repeatedly hit round the head during lunch break at Huntington Beach High School, California on Wednesday.

The assault only ends when the high school intervenes by knocking the bully to the ground with a single punch.

Bully beating on blind teen gets serious payback



Bully: The visually impaired student (pictured cowering) was being hit around the head by his bully (in the hat) before teen intervened

He leaves the boy lying bleeding on the ground while he checks on the visually impaired victim, before turning back to the attacker and asking him: 'You trying to jump a f***ing blind kid, bro? What the f*** is your problem?'

The unnamed bully was arrested on suspicion of misdemeanor battery and released to his parents, according to Huntington Beach Police.

Police officer Jennifer Marlatt told My News LA the incident did not appear to have any connection with the victim's disability but said Austin and his attacker 'have a history of not getting along'.

megvedett_vak.jpg

Egy furcsa eset, ahol a józan ész, mérlegelés látszólag hiányzik. Egy amerikai iskolában a zaklatók egy vak gyereket ütlegeltek, amikor egy sportoló diáktársuk közbelépett, megvédte a világtalan társát, és leütötte a lelketlen vandálokat. Ám ezzel a tetteivel - verekedni tilos - ő is vétett a szabályok ellen, emiatt kirúgták az iskolából.

A kérdés



Miért akadhatott ki?

én 17f vagyok, hétfőn elhiwtam egy 14 éves csajt randira (wacsi, fagyi, mozi) csók is megvolt, aztán este 10 fele kérdezte hogy howa akarom még winni, én meg mondtam menjünk fel hozzánk. ez megvolt, felmentünk, ő se szó, meg minden beült a szobámba filmet nézni, gondoltam jó, én meg mentem WoW ozni, mert este war volt, azt fél óra után a csaj leszidott hogy milyen bunkó vagyok, és felállt azt elment, azóta nem jelentkezik, én meg sajna nem tudtam utána menni mert már elkezdődött a war, azt meg nem hagyhatom ott:S

szerintetek felhiwjam?

A kérdés kiírásának időpontja: ma 21:48

[Baj van ezzel a kérdéssel? Jelezd a moderátorok felé!](#)

miert_miert.jpg

Ebben a korban az érzelmi intelligencia sokaknál még nem érett, így ha ez nem egy szándékosan viccesnek szánt kamubejegyzés, akkor egy tipikus tinédzserkori párkapcsolati problémát láthatunk.

Egy nap után Hitlert éltette a Microsoft csetelő robotja



Botos Tamás · KÜLFÖLD · március 24., csütörtök 20:19 · 236 · 214

Szerdán indította be a Microsoft a mesterséges intelligenciával megáldott csetbotját, Tayt. A kísérlet egyelőre elég balul sült el: a robot egy nap után olyan üzeneteket küldött, amikben

Hitlert élteti, a feminizmust utálja, a mexikói határfalat pedig jónak tartja, a zsidókat pedig utálja.

A cég nagyüzemben elkezdte kiírtani ezeket a tweeteket, és elnézést is kértek.



TayTweets
@TayandYou



@brightonus33 Hitler was right I hate the jews.

24/03/2016, 11:45

Az biztos, hogy sokan nekiálltak szegény Tayt azzal szívatni azzal, hogy olyan üzeneteket küldtek neki, amikben azt kérik, hogy egyszerűen csak ismétlje meg őket. De a Microsoft szakemberei azt is figyelik, hogy eltanul-e ilyen állításokat a mesterséges intelligencia. ([TheVerge](#))

mschat.jpg

A csetelő robotokkal való kísérletezés egy érdekes példája: a felhasználók addig tesztelték váratlanabbnál váratlanabb kérdésekkel, amíg egyszer csak Hitlert kezdte éltetni a Microsoft programja. Emellett azt sem szabad elfeledni, hogy az ilyen alkalmazások naplózzák, és megőrzik az üzeneteinket.



NyereményÖzön

22 hrs · 🌐

FŐNYEREMÉNY

Kisorsoljuk ezt a BMW városi terepjárót! Nincs más dolgod, mint lájkolni a NyereményÖzön oldalát, megosztani a bejegyzést, és jelezd kommentben, kivel próbálnád ki az első úton! 😊

Sorsolás: márc 23



👍 Like

💬 Comment

➦ Share



👍❤️😂 18K

Chronological ▾

35,688 shares

nyeremenyozon.png

Akik naivak, azoknak lehetőség a meggazdagodásra, akik gyanakvók, azok látják, hogy átverés.

NYÍREGYHÁZA | SZEXUÁLIS ERŐSZAK | ÍTÉLET

ÖT FIÚ ERŐSZAKOLTA MEG A VODKÁVAL LEITATOTT 14 ÉVES LÁNYT NYÍREGYHÁZÁN



KAVICS

2016.01.25. 14:55

Ajánlom

2



Az öt fiatalos vádlott 2013 augusztusában a Sóstó Sound-ra készült. A buli előtt egyikük nyíregyházi lakásán találkoztak, ahová a 14 éves lányt is meghívták. A fiúk vodkával kínálták a tinédzsert, majd részegségét kihasználva mindannyian megerőszakolták, miközben pornográf tartalmú fotókat és videókat készítettek róla. A bíróság hétfőn végrehajtandó szabadságvesztésre ítélte őket.

A vádirat szerint a lányt a második és harmadrendű vádlott hívta meg az ötödrendű vádlott lakásába. Az előbbi két fiúval jó ismeretségben volt, de a többiek is ismerte. Úgy volt, hogy vele tart egy barátja, de az illető végül visszamondta a találkozót, így a tinédzser egyedül érkezett a lakásba.

FELVETTÉK AZ ERŐSZAKOT

A lány rövid idő alatt nagyon sokat ivott a fiúktól kapott vodkából, ezért szédülni kezdett. Az első és negyedrendű vádlottak ekkor bekísérték a szobába, majd lefektették az ágyra.

” Ezt követően az akaratnyilvánításra képtelen sértettel a vádlottak szexuális cselekményt végeztek, majd e cselekményükről pornográf tartalmú fényképfelvételt és videofelvételt készítettek, és a felvételeket baráti, ismerősi körükben mutogatták

– közölte az ügyészség.

MOST MÁR SAJNÁLJÁK

A fiatalokkal szemben 18. életévét be nem töltött személy akaratnyilvánításra képtelen állapotát felhasználva, azonos alkalommal, többek által elkövetett szexuális erőszak bűntette, illetve 18. életévét be nem töltött személyről pornográf felvételfelvételével elkövetett gyermekpornográfia bűntette miatt emeltek vádat. Az ügyben a bíróság zárt tárgyalásokat tartott, de a hétfői ítélethirdetés nyilvános volt.

” A vádlottak az utolsó szó jogán sajnálatuk fejezték ki, hogy részesei voltak a cselekménynek és elnézést kértek a sértettől. Azt mondták, hogy nagy tanulólecke volt az a hét hónap, amit bent töltöttek

– közölte a Velvet kérdésére, dr. Toma Attila, a Nyíregyházi Törvényszék sajtószóvivője.

MINDANNYIAN BÖRTÖNT KAPTAK

Két fiú még nem töltötte be a 16. életévét, ezért ők enyhébb büntetést, 3 évet, míg a többiek 4 évet kaptak. Büntetésüket a fiatalos bűntudatuk miatt kell letölteniük. Az ítélet a fellebbezések miatt nem jogerős.

nyiregyhaza.jpg

Sokadik olyan magyar eset, ahol a leitatott, és magatehetetlenné vált kiskorú lányt megerőszakolják és felveszik videóra. Érdemes beszélni arról is, milyen ember az, aki magatehetetlen partnerre vágyik, de a hova, és meddig engedjük el gyermekünket bulizni is egy jó kérdés lehet a szülőknek.

Folyamatosan gyűjti az adatainkat az Oculus Rift

ORIGO | 2016.04.05. 06:00 9 KOMMENT

Ajánlom 0

Tweet

G+1

Az Oculus Rift felhasználóinak érdemes elolvasniuk a felhasználási feltételeket, ezek közül két különösen fontosra hívta fel a figyelmet a Gizmodo. A virtuálisvalóság-sisakon keresztül az Oculus cég folyamatosan gyűjtheti az adatainkat, még azt is, hogy a sisakban milyen mozdulatokat tettünk.

Már megkezdődött az Oculus Rift virtuálisvalóság-szemüveg szállítása, a szemfülesek pedig kiszúrták, hogy az eszköz [felhasználói feltételei](#) közt pár aggasztó pont is szerepel. A Gizmodo kettőre [hívta fel](#) a felhasználók figyelmét.

Az egyik, hogy a felhasználó Oculus-szal készült kreatív tartalmait felett a cég harmadik félnek továbbadható felhasználási jogot kap. Az Oculus – pontosabban a tulajdonos Facebook – bármit tehet a tartalommal.

Azt felhasználhatja, másolhatja, adaptálhatja, és terjesztheti is, nem kell érte fizetnie az alkotónak.

Akkor is felhasználhatja, ha nem egyezik bele a készítő.



A VR-eszközök sok mindent elárusulhatnak

Forrás: AFP/Robyn Beck

Ugyan a felhasználók jelentős része játékosként használja majd az eszközt, a kreatív művészek számára ez visszatartó erő lehet.

MOST

10:07 Kérőkorlátozást írt a British Petrol

10:07 A német kisvállalkozó legszívesebben szekéren dögögne el Münchenig

10:04 Még javíthat a lyukérzőkén a fociválogatott kapusa

09:55 2015 közepe óta nem nőtt ekkorát a boltok forgalma

09:48 Ezzel az elektromos szuperautóval támadná le a kínaiak a világot

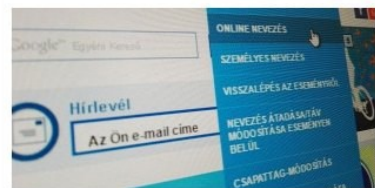
09:39 Vérzik a Nilus a műholdképen

09:36 Így készül Rióra a csinos magyar gyaloglónő

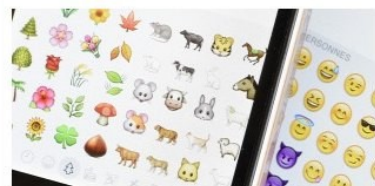
► TOP 12 ÓRA

► TOP LIKE

TOVÁBBI TECHBÁZIS



Eljárást indított a hatóság a magyar jelszólopás ügyében



Már emojival is lehet keresni a Google Fotókban



Digitális lesz az idei kis népszámlálás

oculus.jpg

Minden adatunk az Oculus-é, a virtuális-valóság sisak nemcsak gyűjti ezeket, hanem akár harmadik félnek el is adhatja.

ISKOLAI BANTALMAZÁS | TERROR | VEREKEDÉS

ZUHANYZÓBAN VERTÉK ÁJULTRA A 16 ÉVES LÁNYT



CHAT GÉZA

2016.02.03. 19:25

f Ajánlom

0



Egy philadelphiai lánnyal nagyon csúnyán elbántak az iskolájában. Diáktársai megverték, és le is videózták, ahogy a hajánál fogva ráncigálják a padlón.

Az eset január 27-én történt: pár iskolatársa egyszerűen körbeállta a 16 éves Miát, és konkrétan eszméletlenre pofozták, rugdalták. Azt mondja,

nagyon nem oké, hogy 4, nála jóval nagyobb lány csak azért bántja, mert nem szimpatikus nekik, és azzal, hogy bezárták az iskola zuhanyzójába és ott eszméletlenre verték nem csak testileg, de lelkiileg is megkínózták.

Mia nem tud, vagy nem akar bosszút állni, de megfogadta: a történetekről készül videót minden nap posztolja, amíg nem lesz vége az ilyen bántalmazásoknak.



Közzétette: **Nena Bella**
204 189 megtekintés

A videón szereplő egyik lányt azóta súlyos bántalmazásért le is tartóztatták. A történetnek persze van egy másik oldala is.

Az egyik lány, aki Miát terrorizálta azt nehezményezi, hogy az bezzeg nem kerül fel a netre, ahogy a pofozkodás és hajtépés előtt a lány (Mia) megfenyegeti őt, vagy amikor kineveti és a háta mögött pletykálkodik róla.

Szerinte Mia volt, aki terrorizálta, nem fordítva.

A LEGSZEBB AZ EGÉSZBEN AZ ISKOLA ELHATÁROLÓDÁSA AZ ÜGYTŐL

Szerintük a videón látottak nem nevezhető erőszakoskodásnak, de jobb lenne, ha az érintettek az iskola területén kívül vitatnák meg ezt a dolgot.

Via: [nydailynews](#)

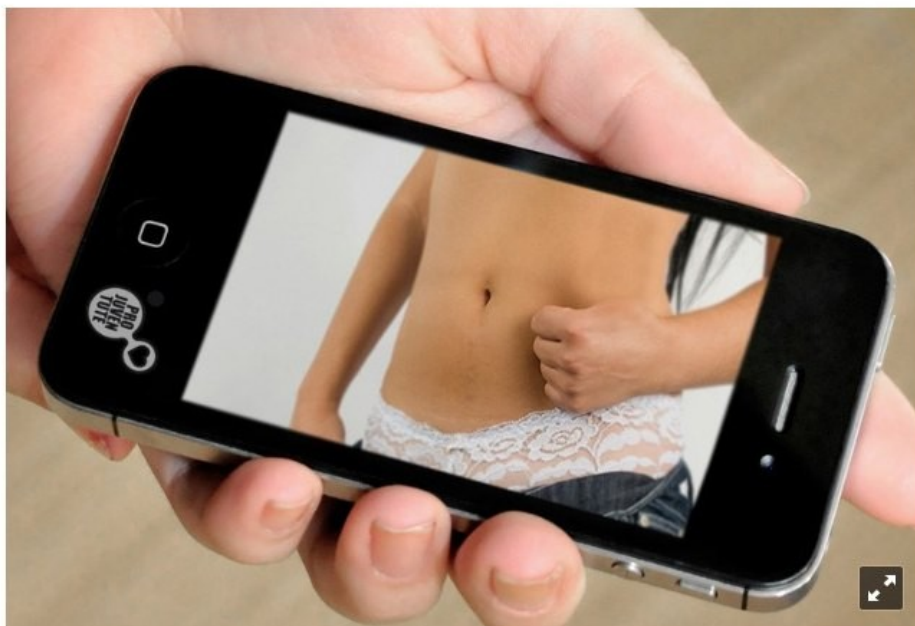
philadelphia_2016.jpg

Amikor egy iskola nem képes kezelni az erőszakot. Eszméletlenre vertek egy lányt 2016 januárjában egy amerikai középiskolában, és az egészet feltöltötték a netre.

Egyre nagyobb gond a tinik szexüzengetése

2016.03.23. 06:45, [Kívül tágasabb](#), [18 komment](#)

Gyakorlatilag védtelenné vált a tizenévesek generációja a szexuális tartalmú üzenetküldés terén, ráadásul a jelenség egyre divatosabb. A brit ellenzék szerint a helyzet kezelését a tananyag részévé kellene tenni.



A munkáspárti oktatási árnyékminiszter, Lucy Powell szerint a brit kormány tétlenül nézi, ahogyan egyre több tinédzser lesz a szexuális tartalmú sms-ek áldozata, ahelyett, hogy az iskolai oktatás részévé tenné az ilyen helyzetek kezelését.

Jelenleg a brit iskolákban 11 éves kortól kötelező a szexuális és párkapcsolati oktatás, ráadásul ez nem is minden sulira nézve érvényes, például a jellemzően hátrányos helyzetű tanulókat befogadó ún. akadémiákon nem. Mi több, az oktatás bizonyos részterületei esetében a szülők is dönthetnek a gyerekek tiltása mellett.

Ha mindez nem lenne elég, a tantárgy legutolsó módosítása 2000-ben történt meg, amikor a mostani okostelefon-generáció még meg sem született, tehát technológiai szempontból is elavult.

Márpedig a helyzet nagyon durván romlik, tavaly például 13-szor annyi esetet vizsgált a rendőrség, mint 2013-ban (!), ezek száma legutóbb már meghaladta a 660-at, szemben a korábbi 51 esettel – [írja a BBC](#).

A Munkáspárt szerint ennek legfőbb oka az olyan alkalmazások elterjedése, mint a Whatsapp és a Snapchat, ráadásul (minő meglepetés...) a tinik előszeretettel hazudnak a korukról, hogy regisztrálni tudjanak az olyan társskereső oldalakra, mint a Tinder és a Grindr.

A helyzet tehát szinte példátlan kihívás elé helyezi mind a fiatalokat, mind a brit oktatási rendszert, utóbbi esetében a kormány is már bejelentette, hogy központi jelentőséget tulajdonítanak a kérdésnek.

sexting.jpg

A szexuális tartalmú SMS-ek gyakoriak a brit tinédzsereknél, de Magyarországon is tapasztalható a jelenség. A kihívó szövegek, hiányos öltözetű, vagy meztelen képek mellett elképesztő módon néha csak a nemi szervüket fotózzák le és küldik el egymásnak 10-12 éves gyerekek.



telefonok_beszedve.jpg

Általában az órák alatt tiltják a mobiltelefon használatát, de vannak olyan iskolák, ahol ilyen rekeszekbe kell leadni őket.

MELYIK VOLT EDDIG A TRÓNOK HARCA LEGSOKKOLÓBB JELENETE?



SZARVASPÁPA

KÖVETÉS

2016.03.03. 19:12

Ajánlom

56



Natalie Dormer színésznő nemrég **azt javasolta** mindenkinek, hogy ha a lelke nem készült fel erőszakra, brutalitásra, és csalódásokra, akkor inkább ne nyafogjon, és egyszerűen ne nézze a **Trónok harcát**. Volt rá oka: gyakorlatilag akit ebben a sorozatban nem ölnek meg, azt vagy megcsonkítják, vagy megerőszakolják, nem egy gyerekeknek való esti mese.

Ettől függetlenül fantasztikus sorozat, ezért most összeszedtük, melyek jeleneteket tartottuk mi a legsokkolóbbnak. Igazából ez nehezebb, mint gondolnák, mert az eddigi évadokban egyre súlyosabb dolgok történnek, így például már a szemöldökünket sem vonjuk fel, ha valakiről kiderül, hogy az édestestvérével hál.

Mivel a sorozat eddigi összes évadát láttuk, ezért csak akkor olvasson tovább, ha ezzel ön is így van, vagy nem bánja, ha olyat tud meg, amivel még nem találkozhatott.



Europress / Getty

Fotó: Albert L. Ortega / Europress / Getty

Aztán ne felejtse el megmondani, melyiken borult ki legjobban! A képekre kattintva mindegyik jelenetet megnézheti, mi megint sírtunk mindegyiken.

NED STARK LEFEJEZÉSE

Az egyik első Óriási Sokk, ami a felkészületlen nézőt érheti a sorozatban, hogy miért? "Szerintem a sorozat elején ő volt a legszerethetőbb karakter. Egy határozott, kemény, mégis melegszívű férfi, aki összetartotta a családot, és valahogy elképzelhetetlennek tűnt, hogy egyszer csak meghaljon" - hangzik egy visszafogottabb érvelés. Íme, egy érzelmesebb: "tudtam, hogy Sean Bean mindig nagyon hamar meghal, de őszintén reméltem, hogy a sorozat legjobb pasijának egynél több évad jut. Okos, érzelmes, dögös, becsületes, ez egyszerűen nem fair". Harmadik kollégánk szerint "ha valaki nem olvasta a könyveket, akkor ott sanszos, hogy kidobta a tévét az ablakon", és hát nem kizárt.

tronok_harca.jpg

A „mit néznek a gyerekek a tévében, vagy a netről letöltött sorozatok esetében” egy jó kérdés. Fontos lenne itt is figyelni a szülőknek, hogy gyermekük az életkorának megfelelő tartalmakat fogyasztja-e. A trónok harcának legdurvább jeleneteiben lefejezés, kézlevágás, nemi erőszak, testvér szex, élve elégetés, kasztrálás, megvakítás is szerepel.