



GYERMEKEINK VÉDELMEBEN

Hogyan vigyázzunk rájuk még jobban?

Sorozatunk huszonegyedik epizódjában igyekszünk néhány jó tanácsot adni a kisgyermekes szülőknek és a fiataloknak. Gyermekeinket nagyon szeretjük, nem szeretnénk, hogy bántódásuk essen, azonban tapasztalatlanságuk és naivitásuk miatt kiemelt célpontjai az internet bűnözőinek. Cikkünkben bemutatkozik a NOD32 sokak számára egy vadonatúj oldaláról, illetve ismertetjük a szülői felügyelet egy lehetséges módját az új 4.0 változat segítségével.

Sokan esnek abba a hibába, hogy alábécsülik a szülők viselkedésének mintaadási funkcióját. Pedig óriási jelentősége van. Ha például a gyerek rendetlenséget lát a szülő íróasztalán, lehet, hogy hiába kérleljük majd a játékpolic elpakolására. De ugyanígy érdemes – persze a saját korának megfelelően – válaszolni is a kérdéseire az egyszerű tiltások helyett, amelyek értetlenségre, „csakazértis”-típusú dacról vezethetnek. Meg kell érteni vele, miért nem tesszük közszemlére az összes személyes adatunkat, mik

a veszélyei a bárki által nézegethető kihívó, fürdőruha képeknek, milyen honlapoktól jobb, ha óvakodik stb. Persze ez a nehezebb út, sok türelmet igényel, de hosszú távon mindenképpen célravezetőbb. Fussuk át először is a legfontosabb, biztonság-gal kapcsolatos területeket, hiszen sokszor maguk a felnőttek sem érzékelik a veszélyforrásokat.

Autorunos eszközök

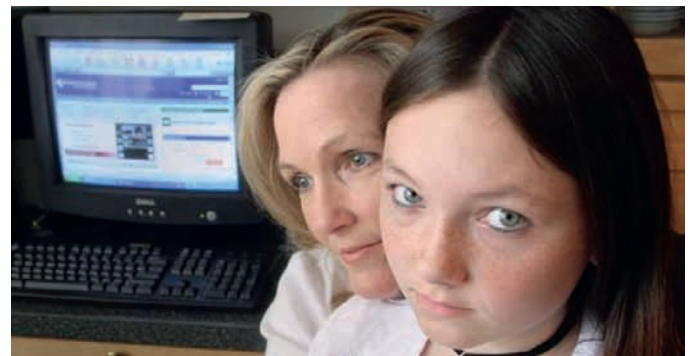
Sok gyerek használ MP3-as, MP4-es zenelejátszót, de az USB-kulcsok, fényképezőgépek,



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 a mintegy 226 millió tagot számláló hálózatban



Van, akinek tetszik, van, akinek furcsa, hogy számos online híroldalon is iskolás lányok képe néz az olvasóira. Ha a szülő tud róla, és megengedi, akkor persze más a helyzet, de kérdés, hogy valóban így történik-e az esetek többségében



A számítógép-használat és az internetezés életünk részévé vált. A szülők csak akkor tudják megvédeni gyermeküket a veszélyektől, ha azok természetével saját maguk is tisztában vannak

memóriakártyák mind-mind képesek arra, hogy a számítógéphez való csatlakoztatáskor automatikusan futtassanak egy adott állományt. Ha viszont az eszköz fertőzött valamilyen INF/Autorun típusú vírussal, akkor megfertőzheti a számítógépünket is. Érdemes lehet emiatt valamiféle vírus- és kémirtó programot hasz-

nálni, a gyerekekkel pedig megértetni, hogy a zenelejátszóját ne „tölts fel” mindenféle ismeretlen számítógépen.

Ki ül a másik gépnél?

Nem mindenki az, akinek látszik. A közösségi oldalakon is vannak olyan rejtőzködő bűnözők, pedofilok, akik adatlapjuk alapján lát-



A kisebb gyermekeket is fel kell világosítani arról, hogy sosem lehet biztosan tudni, kivel folytat éppen beszélgetést. Ha például a chatpartner meztelen fotót kér, vagy a ház riasztójának kódja után érdeklődik, az már a szülő haladéktalan közbeavatkozását igényli

szólag gyerekek, de valójában az a céljuk, hogy kikérdezzék, és behálózzák a gyanútlanabbakat, akár az elkotyogott információkkal történő zsarolással.

Sose adjuk meg minden személyes adatunkat a közösségi portálokon, mert mások visszaélhetnek velük! 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.

Link üzenetek

Léteznek olyan kártevők, amelyek a Live Messenger üzenetein keresztül terjednek, és abban egy linket kapunk egy ismerősünktől.



Egy áprilisi felmérés szerint a munkavállalók több mint fele (egészen pontosan 62,8 százalékuk) ad meg magáról túlságosan részletes személyes információt a közösségi portálokon, amellyel közvetve már a munkaadók érdekeit is veszélyeztetik

Azonban ha rákattintunk, egy kártevő terjesztő oldalra kerülünk, amely megfertőzheti a számítógépünket.

Sose kattintsunk olyan linkre, amely váratlanul, esetleg csak angol nyelvű üzenettel érkezik, és még akkor se tegyük ezt, ha ezt látszólag a barátunktól kaptuk!

Semmi sincs ingyen

Sok weboldalon, torrentszerveren található feltört programok, mobiltelefonok függetlenítését végző segédprogramok, szériaszám-generátorok. Azonban ez egyben ideális terep a bűnözőknek, akik a legújabb vírusokat, férgeket, kémprogramokat tesztelik a gyanútlan áldozatokon. Óvakodjunk a warez tartalmaktól, ezekben sokszor olyan kódok bújhatnak meg, amelyek a legfrissebb kártevőket tartalmazzák. Ráadásul a törvényeket is megsértjük, ha ilyeneket töltünk le torrentszerverekről, hiszen a folyamattal egyben feltöltőkké is válunk!

A statisztikák is ezt mutatják

A Webroot egy átfogó felmérés keretében mintegy ezregerősség Facebook-, MySpace-, Twitter-LinkedIn-felhasználót kérdezett ki a webhasználati szokásaikról. Az eredmények alapján elmondhatjuk, az óvatosság sajnos nem igazán jellemző.



Nemcsak titkos ügynökök, de a Microsoft vezetőjét is megtalálhatjuk részletes adatokkal, családi fotókkal. A publikus adatokkal kapcsolatosan szinte mindenkinél nagyobb odafigyelés lenne szükséges

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, egyenyedük (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 között a fiatalok számítanak a legvesélyeztetettebbnek, az átlagos 28 százalékos értékkel szemben 40 százalékuk fogad el barátkérőt idegentől, és náluk sokkal jellemzőbb az összes személyes adat, elérhetőség megadása is.

Jól látható, hogy a közösségi oldalak egyre inkább a kártevő-terjesztők célkeresztjébe kerülnek. Kártevők, csalások, hamis linkek, átverések ugyanúgy kifizetődnek itt is, mint az átlagembereknek küldött adathalász levelek: elegendő csak 5 százalék, aki lépre megy, és a tetteseknek már bőségesen megéri. Mi mást is javasolhatnánk végül, mint a személyes adatok ésszerű korlátozását, gyanakvást az idegenekkel szemben, rendszeres frissítéseket, biztonsági szoftverek használatát, valamint egyedi jelszavak alkalmazását mindenhol.

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeney@pcworld.hu).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus
magyarországi képviselője
antivirus.blog.hu

KAPCSOLÓDÓ WEBOLDALAK

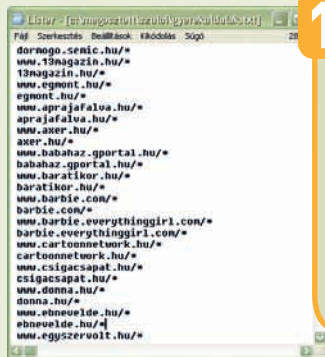
www.eset.hu/szuloifelugyelet

Hogyan hozzunk létre felhasználói fiókot Windows XP-n gyermekünknek:
hopp.pcworld.hu/6082

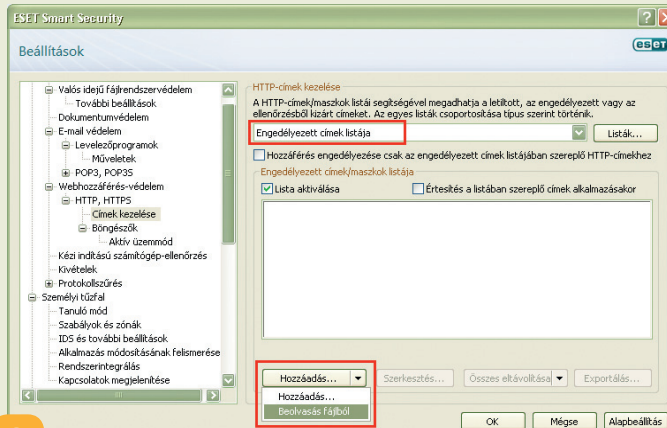


SZÜLŐI FELÜGYELET WEBBÖNGÉSZŐHÖZ, 6 LÉPÉSBEN

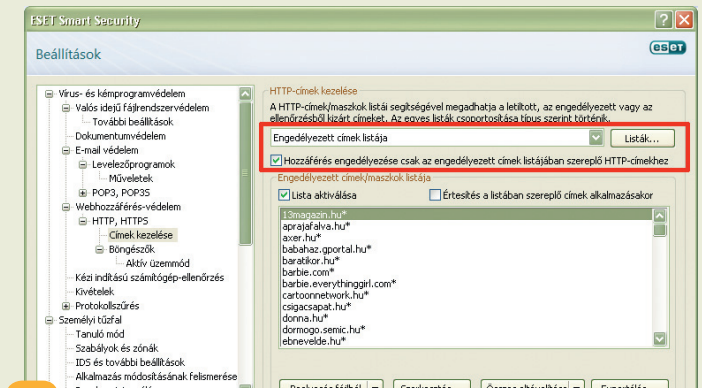
Mielőtt belekezdünk, érdemes leszögezni, hogy tökéletes, kijátszhatatlan szülői felügyeleti szoftver nem létezik. Ez a mostani sem az, de megkísérel segíteni, hogy gyermekünk csak a neki szánt weboldalakhoz férhessen hozzá internetezés közben.



1 Töltjük le, és mentjük el számítógépünkre a legnépszerűbb, gyermekeknek szánt internetes weboldalak listáját. Ezt a www.eset.hu/szuloifelugyelet oldalon találhatjuk meg. A válogatás egy olyan alap linkgyűjtemény, amelyet a Siccontact Kft. állított össze a gyermekek internetezési szokásait vizsgálva.

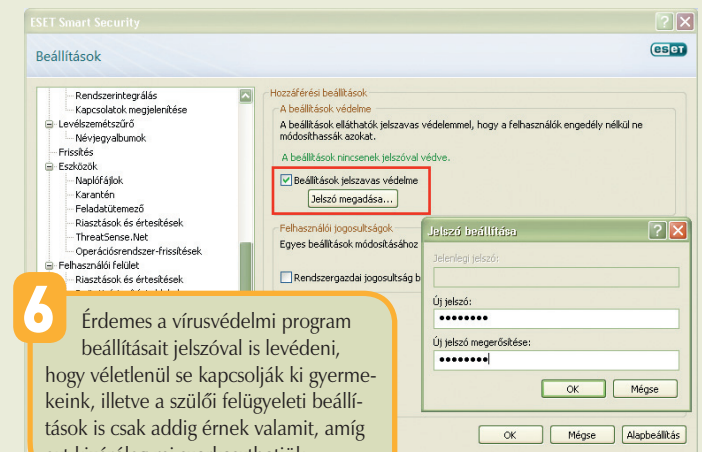


2 Nyissuk meg az ESET Smart Security vagy az ESET NOD32 Antivirus beállítási fáját az [F5] billentyű megnyomásával, és válasszuk ki a **Vírus- és kémprogramvédelem** → **Valós idejű fájlrendszervédelem** → **Webbongás-védelem** → **HTTP, HTTPS** → **Címek kezelése** beállítási lapot.



4 Jelöljük be a **Hozzáadás engedélyezése csak az engedélyezett címek listájában szereplő HTTP-címekhez** opciót, majd a beállítások mentéséhez nyomunk OK-t. Ezzel már érvénybe is lépett a szűrési üzemmód.

3 Az **Engedélyezett címek listája** tétel kiválasztása után jelöljük ki a **Hozzáadás** → **Beolvasás fájlból** menüpontot, és olvassuk be az imént lementett, és igényünk szerint tovább módosított URL-listát.



6 Érdemes a vírusvédelmi program beállításait jelszóval is levédeni, hogy véletlenül se kapcsolják ki gyermekeink, illetve a szülői felügyeleti beállítások is csak addig érnek valamit, amíg azt kizárólag mi szerkeszthetjük.

5 A szűrés bekapcsolása után biztosak lehetünk abban, hogy gyermekünk már csak a listán szereplő weboldalakat tudja látogatni. Az engedélyezett tételeket igény szerint bármikor bővíthetjük, törölhetjük vagy módosíthatjuk a későbbiekben.