MIT LÁT AZ INTERNET BELŐLÜNK?

Tudom, ki vagy!

Sorozatunk huszonhetedik epizódjában többek közt azon fogunk elmélkedni, hogy milyen nyomokat, adatokat hagyunk magunk után az interneten, mit lehet rólunk kideríteni. Vajon hibáztunk-e valamit, ha túl sok tudható meg rólunk? És amit mi látunk másról, az vajon igaz-e? Ez már csak azért is érdekes kérdés, mert egy ilyen búvárkodás nem csupán jó szándékkal történhet. Megvizsgáljuk azt is, hogy vajon az elkerülhetetlen-e, hogy szórakozott idióták, ismeretlen spamküldő emberkék kéretlen, gyanús és néha fertőzött oldalra mutató linkeket küldözgessenek nekünk kedvenc csevegőprogramjainkban.

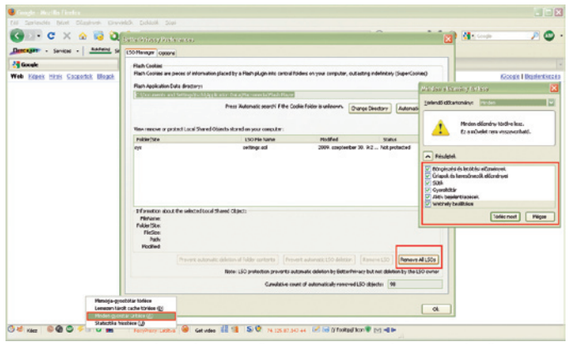
Cikksorozatunkban már sokszor és sokat beszéltünk arról, hogy a közösségi oldalakon érdemes okosan és mértéktartóan adatokat szolgáltatni magunkról. Erről legutóbb a 24. részben is szó esett, az egyik elrettentő példa pedig pont az MI6 brit titkosszolgálat főnökének felesége volt, aki óvatlanul még a lakcímüket is közzétette a Facebookon. Vagyis kiindulhatunk abból, hogy ha óvatosak akarunk lenni, akkor a frissített windowsos gépünkön semmilyen alapvető hibát nem ejtünk: a biztonsági frissítések automatikusan érkeznek és településünk, sőt vírusirtónk és kémprogramirtónk is naprakész állapotban van, valamint felhasználói szokásainkban is igyekszünk megfontoltak lenni. Akkor hát meg is úszunk mindent?

Nem biztos, egyrészt már rögtön benne van a pakliban az is, hogy nem létezik százszázalékos védelmi program. Egy vadonatúj kártevő pedig még a legjobb vírusirtó használata mellett is „bekapható". De emellett az internetes programjaink beállításaival is sokat lendíthetünk vagy ronthatunk biztonságunk kerekén.

Nincsenek titkaink!

Az előző, 26-os epizódban már adtunk pár tanácsot a böngészéshez, és megemlítettünk pár hasznos plugint is. Ha például arra koncentrálunk, hogyan használjunk banki szoftvereket, akkor kialakíthatunk egy biztonságos ügymenetet: a bank weboldalának címét mindig magunk gépeljük be, sose használjunk ehhez e-mailben érkezett linket. Indulás előtt az esetleges korábbi böngészés után végezzünk cache-ürítést, töröljük a korábbi munkamenetekhez tartozó session cookie-kat és az átmeneti állományokat. De vajon elég-e mindez? Nos, ennek eldöntésére végezzünk el egy kísérletet.

A What the Internet Knows About You weboldal (**whattheinternetknowsaboutyou.com**) érdekes dolgokat mutat meg nekünk. Elemzi a böngészőnkben megbúvó adatokat (History, CSS, DOM) információkat, előzményeket, és elég alaposan feltérképezi, merre jártunk. Érdemes megfigyelni, hogy a detektálás annak ellenére igen sikeres, hogy a NoScript és további biztonsági pluginok aktívak. A böngészési előzmények tartalmazhatják a közösségi oldalakon levő (Twitter, Facebook, MySpace stb.) ismerőseinket, a rendszeresen látogatott banki oldalakat, a használt keresőket (Google, Yahoo, Bing, AllTheWeb stb.), valamint a felnőtt tartalmak és kormányzati oldalak, illetve a Wikileaksen tett látogatásaink nyomát is. Ha már eléggé kiborzongtuk magunkat, elolvashatjuk a How it works (hogyan működik), a Tech details (technikai részletek), valamint a Solutions (tippek a felhasználók számára) menüpontot is. Ebben megtudhatjuk, hogy a böngésző előzményei (History) körül hogyan tehetünk ellenlépéseket. Telepíthetjük például a Link Status (**addons.mozilla.org/en-US/firefox/addon/12312**), illetve a SafeHistory (**www.safehistory.com**) pluginokat Firefox alatt (utóbbi sajnos csak a 2-es Firefox széria alatt működik). Ha a What The Internet Knows About You lekérdezését úgy indítjuk el Firefox alól, hogy ezek és a kedvenc NoScript (**addons.mozilla.org/addon/722**) kiegészítőnk is fent vannak, előtte pedig töröljük a hagyományos és Flashsütiket, az átmeneti tároló (cache) tartalmát, az előzményeket és a munkameneteket, úgy alig vagy semmit sem fog találni a weboldal.



Ha bankolni szeretnénk, jó ötlet előtte az összes további böngészőablak bezárása, a cache ürítése, valamint a BetterPrivacy (addons.mozilla.org/hu/firefox/addon/6623) plugin segítségével még a Flash cookie-k törlése is. Sok webhely pontosan ez utóbbi segítségével állítja elő a hagyományos előzmények és egyéb személyes adatok törlése után a felhasználói szokásainkat leíró adatbázist

Mint egy citromot, úgy facsarja ki a What The Internet Knows About You weboldal a böngészőnkben megbúvó adatokat. Érdemes megfigyelni, hogy a detektálás annak ellenére igen sikeres, hogy a NoScript és további biztonsági pluginok aktívak. Inkább buli ez, mint igazi forensic eszköz, de tud érdekes meglepetésekkel szolgálni, annyi bizonyos

Ezzel vissza is érkeztünk a bankolás témaköréhez, amit szeretnénk a legnagyobb biztonságban tudni. Láthattuk, hogy ha bizonyos lépéseket megteszünk a kémkedő internetes „csodaweblap" ellen, akkor ezek használnak, és ugyanígy érdemes a pénzügyi tranzakciók környezetét is biztonságosabbá tenni. Persze mint mindent, ezt is tovább lehet fejleszteni; például linuxos Live CD-s rendszerindítású Firefox használattal, vagy egy külön virtuális gépben (Sun VirtualBox, VMware Player, Microsoft Virtual PC) történő Linux-indításhoz is felkészülhetünk. Ez utóbbi előnye az lehet, hogy ott már kedvenc beépülőinket is fel tudjuk telepíteni, és ezt a jól testre szabott konfigurációt csak erre a célra használhatjuk. Azért persze ilyenkor se felejtsük el, hogy ellenőrizzük a banki weboldal tanúsítványának érvényességét, a ShowIP (**addons.mozilla.org/en-US/firefox/addon/590**) plugin pedig megsúgja, hogy a szokásos IP-címen látogatjuk-e éppen kedvenc bankunkat. Ha nem a favicon helyén szereplő lakat ikont nézzük be tévesen, úgy erőfeszítéseink nem lesznek hiábavalóak, és pénzünk, jelszavunk hosszú ideig csak a miénk maradhat.

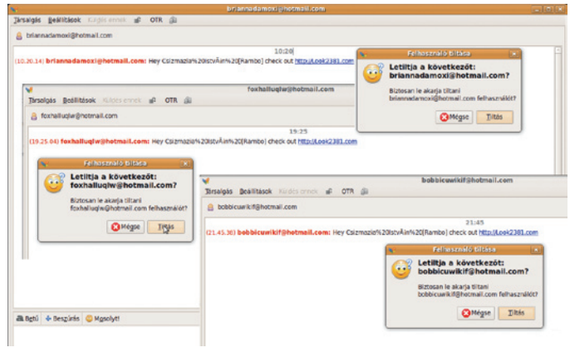
Harmadik és „legolcsóbb" módszer Windowson a Firefox Portable (**portableapps.com**) alatti, csak bankolásra összerakott böngészőkörnyezet használata, ezt akár egy pendrive-on magunkkal is hurcolhatjuk.

Balekok, rajongók, csalók, megtévesztők

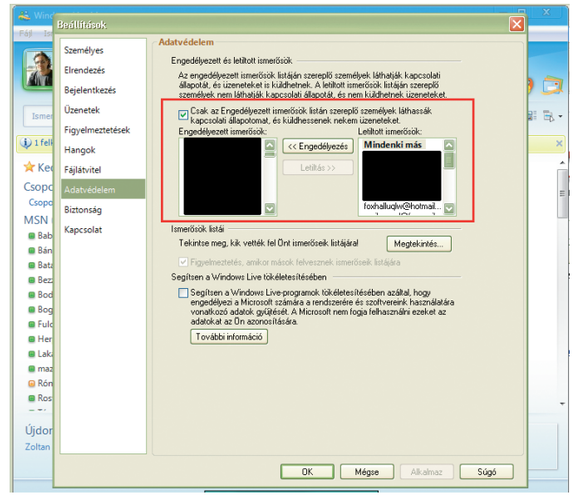
Amikor egy ismerősünket keressük, vagy egy érdekes ember mikroblogjára szeretnénk követőként feliratkozni, nem árt alaposan megnézni, valójában kinek az adatlapját is nézzük éppen.

Nem ritka ugyanis, hogy egy-egy nagy név mögött nem az van, akinek a neve oda van írva. Sőt, a gyakori nevekből, vagy a híres emberekből több tucatnyit is találhatunk, például az Ubuntu disztribúció készítőjének nevével is visszaélnek tömegesen a Twitter-felhasználók. Persze lehetünk annyira megengedők, hogy némely **Mark Shuttleworth** esetében jótékonyan esetleges névazonosságot is feltételezhetünk. Ennél is tovább mennek egyesek, ha például **Bill Gatest** keressük, nyomban temérdek ilyen nevű szereplő tűnik elő, közülük jó néhányan pedig ráadásul hamis fotóval adják ki magukat másnak, mint akik valójában.

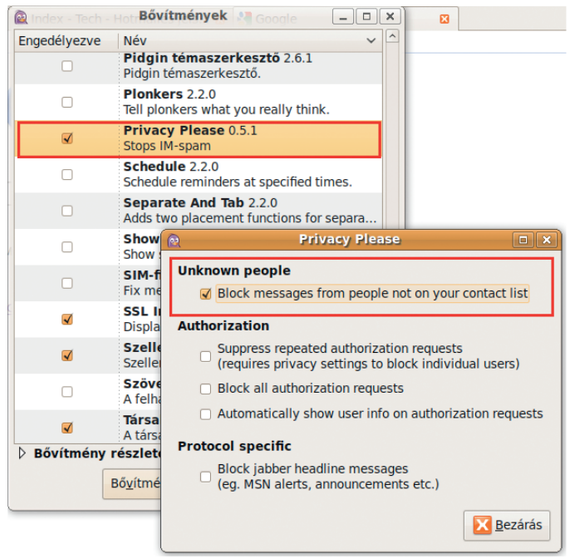
A Facebook esetében a híres emberek köré néha rajongói kört szerveznek, így itt sokszor könnyebb felismerni a sok szereplő között, hogy valójában ki is az igazi. Ezt továbbgondolva kimondottan kellemetlen forgatókönyv lehet azonban, ha valaki a nevünkkel visszaélve – esetleg a közösségi oldalunkról kinézett személyes adatainkat felhasználva – lejáratóblogot indít valaki vagy valami ellen a nevünkben. Éppen idén augusztusban indult el egy per egy blogger ellen, aki **Liskula Cohen** topmodellről írt állítólag kedvezőt-



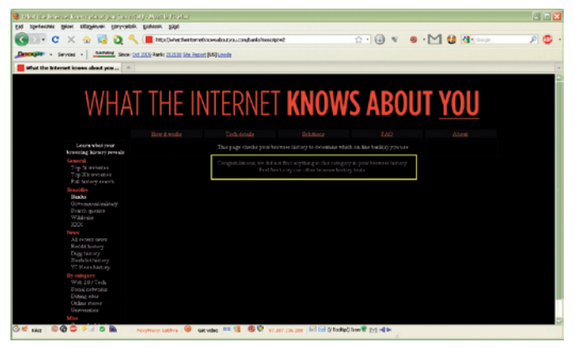
Egymás után pattannak fel az MSN-ablakok, benne ismeretlen partnerek invitálnak gyanús oldalakra. Ha nem akarjuk, nem szükséges minden sudribunkóval polemizálni, a leghelyesebb, ha már be sem engedjünk őket a privát szféránkba



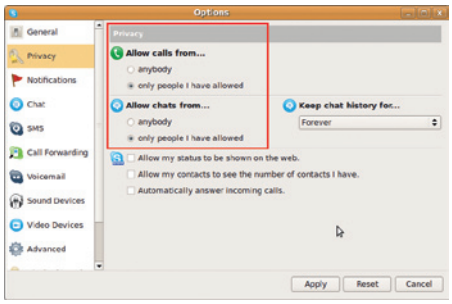
A Windows Live Messengerben meg kell keresni az Adatvédelem menüpontot, és máris elhelyezhetjük a pipát a Csak az engedélyezett ismerősök listán szereplő személyek küldhessenek nekem üzeneteket pont mellett. Viszlát, kéretlen spam üzenetek, ha nem írunk, ne válaszoljatok!



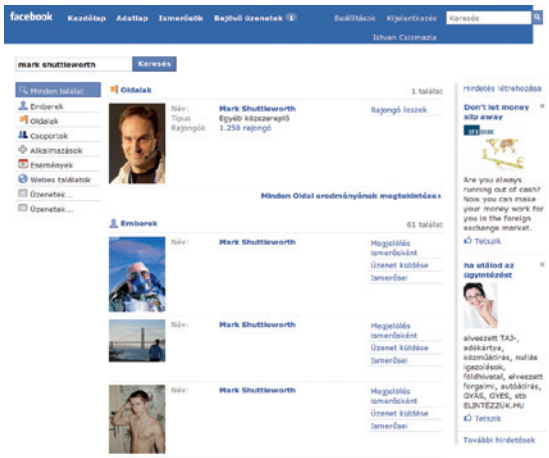
Ugyanez egy Linux alatt futó Pidgin esetében. Ez ugyanúgy képes kezelni az MSN Live profilt, de a kéretlen partnereket ezúttal a Privacy Please nevű pluginnal tudjuk örök hallgatásra bírni. A nyílt forráskódú Pidgin (www.pidgin.im) Linuxon, Windowson és Mac OS X-en is használható



Ilyet is lehet látni, de ez a legritkább eset. Ha előzőleg minden előzmény, cache, hagyományos és Flash cookie, illetve egyéb személyes adat törlésre került, akkor van csak esélyünk ilyen üzenetet látni a What The Internet Knows About You oldalán



Az MSN Live esetében alkalmazott partnerek tiltása természetesen Skype alatt is létezik. Az, hogy ismeretleneknek nem engedjük a telefonhívást, manapság evidencia. A gyanakvóbbak beállíthatják ugyanezt a chatablakra is, kérjen engedélyt a másik, majd akkor diskurálunk vele. Vegyük észre, hogy a státuszunk mutatását, partnereink számának megtekintési lehetőségét és az automatikus hívásfogadást is érdemes letiltanunk

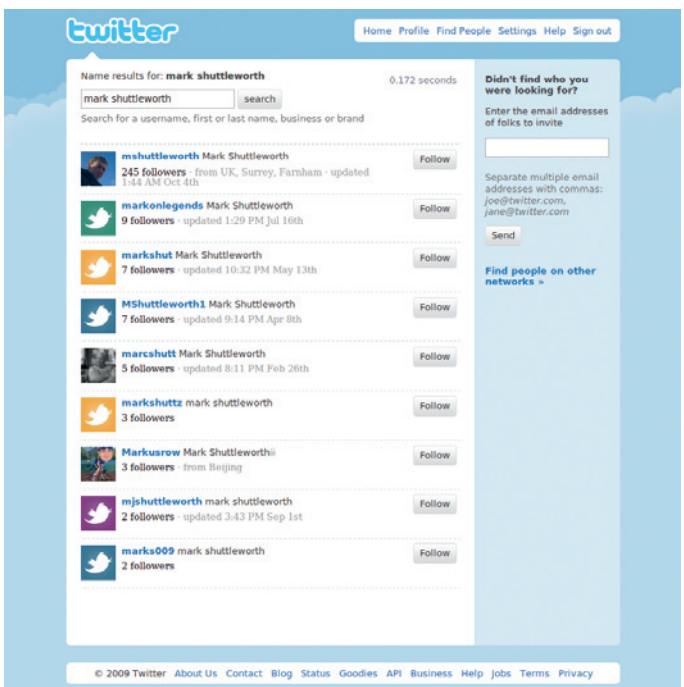


A Facebook esetében a híres emberek köré néha rajongói kört szerveznek, így itt sokszor könnyebb felismerni a sok szereplő között, hogy valójában ki is az „Igazi Trebitsch"

lenül, és emiatt milliós perrel fenyegetik.

Ki küldözgeti ezt nekem?

Nem, ezúttal nem a klasszikus spam levelekről lesz ismét szó. Ezek ugyan nem tűntek el sajnos, de jött mellé új módi: a közösségi oldalakon küldözgetett változat. A szerencsésebbek ezt még hírből sem ismerik, a kevésbé szerencsések hetente kapnak egy-egy ilyet, a kifejezetten pechesek pedig akár naponta többet is. Nos, nekünk sikerült bekerülni ez utóbbi csoportba. Hogy ez pontosan hogy történt – magyarán a spamküldözgető emberekhez hogyan került oda a címünk –, csak találgathatjuk. Az egyik legvalószínűbb forgatókönyv az, hogy valamelyik partnerünk gépe (egyszer) megfertőződött, és ekkor került a címlistája illetéktelen kezekbe. Az ilyen lopott címgyűjteményeket aztán az e-mail címek listájához hasonlóan összeszedik, adják-veszik, és tolják rajta a kéretlen reklámokat, ahogy a csövön kifér. Vagyis szó sincs random telefonszám-tárcsázáshoz hasonlóan véletlenül kitalált felhasználónévre írt üzenetküldésről, hanem csak „megtekerik a kurblit" és az összegyűjtött fix címlista tagjai naponta foghatják a fejüket. Nos, mi szeretnénk elhessegetni az ilyen kéretlen linkajánlókat. Tegyünk hát ellenük valamit! Az egyik nyilvánvaló módszer az, ha nem használunk ilyen csevegőalkalmazásokat. De mi lehetne a másik?



Könnyű lépre menni, mert az internet sincs tele Grál-lovagokkal. Itt az Ubuntu disztribúció készítőjének nevével élnek vissza tömegesen a Twitter-csatornák

Elhárítás MSN-en és Skype-on

Aki már régóta használ számítógépet, az tudhatja, az alapértelmezett (default) beállítások ritkán egyeznek meg az optimális és hatékony beállításokkal. Ahogyan például – jogi okok miatt – a NOD32 és ESS programokban a felhasználóknak kell kézzel bejelölniük, hogy a kéretlen alkalmazásokat és a veszélyes szoftvereket is szűrni akarja-e, ugyanígy érdemes a csevegőprogramok konfigurálására is szánni egy kis időt.

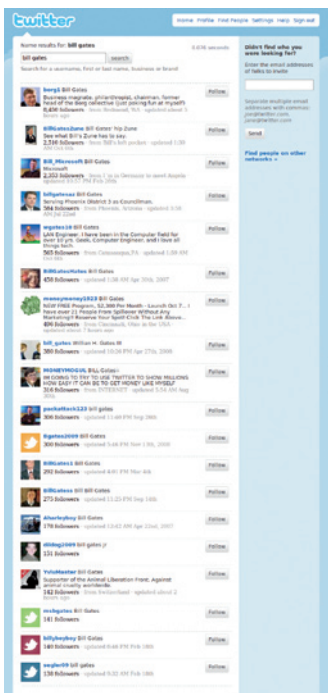
A Windows Live Messengerben meg kell keresni az Adatvédelem menüpontot, és máris elhelyezhetjük a pipát a Csak az engedélyezett ismerősök listán szereplő személyek küldhessenek nekem üzeneteket mellett. Ugyanez a szabad forrású Pidgin esetében is természetesen könnyen megvalósítható. A Pidgin (**www.pidgin.im**, korábban Gaim) képes kezelni többféle, köztük az MSN Live profilt is, de a kéretlen partnereket itt egy külső modullal, a Privacy Please (**code.google.com/p/pidgin-privacy-please/**) nevű pluginnal bírhatjuk örök hallgatásra. A Pidgin további érdekessége, hogy Linuxon, Windowson és Mac OS X-en is egyaránt elérhető.

Az MSN Live esetében alkalmazott partnerek tiltása természetesen Skype alatt is létezik. Az, hogy ismeretleneknek nem engedjük a telefonhívást, az manapság már szinte evidencia. A gyanakvóbbak pedig beállíthatják ugyanezt a chatablakra is: kérjen engedélyt a partnerünk, csak akkor diskurálunk vele. Vegyük észre, hogy a pillanatnyi státuszunk idegeneknek való megmutatását, partnereink számának megtekintési lehetőségét és az automatikus hívásfogadást sem engedheti meg magának egy kellően paranoid felhasználó.

***

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

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



Ennél is tovább mennek egyesek: ha például Bill Gatest keressük, temérdek ilyen nevű szereplő tűnik elő, közülük jó néhányan pedig ráadásul hamis fotóval adják ki magukat a Microsoft alapítójának