MEGTÉVESZTŐK ÉS MEGTÉVESZTETTEK

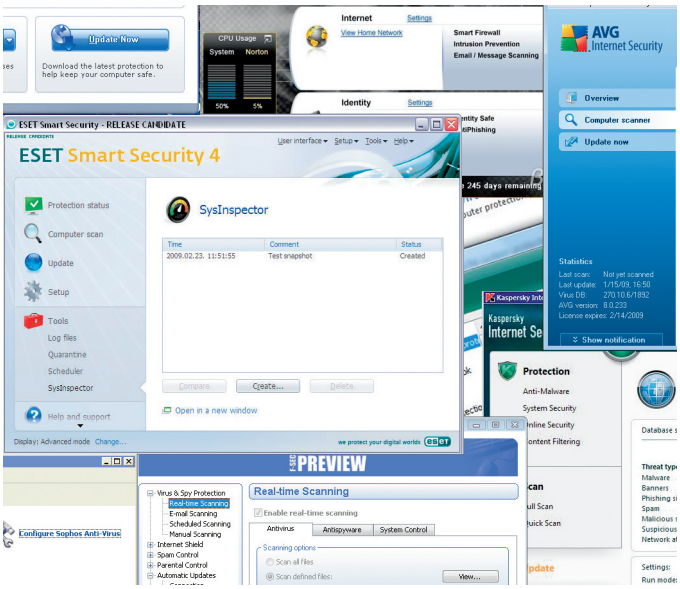
Újabb social engineering fejezetek

Sorozatunk elérkezett a huszadik részhez. Ezúttal ismét a social engineering, azaz a megtévesztés vizeire evezünk. Egy röpke pillanatra visszanyúlunk a történelmi korokba, hogy utána rögtön a legfrissebb csalási módszereket, trükköket tekinthessük át.

A trójai falovak manapság már messze gyakoribbak, mint Homérosz korában, napjainkban leginkább számítógépeinket támadják. Ezek a trójaiak olyan programok, amelyek valami mást csinálnak, mint amit magukról eredetileg állítanak. Ez a „más” nem minden esetben okvetlenül romboló vagy káros, de sok esetben igen: az ilyen szoftverek fájlokat törölnek, felülírják a merevlemezt, vagy távoli hozzáférést biztosítanak a rendszerhez a támadónak. Egy klasszikus trójai általában tartalmaz egy billentyűleütés-naplózót (keylogger) is, amelyet készítői játéknak vagy valamilyen hasznos segédprogramnak álcáznak. Az efféle trójaiakat sokféle céllal alkalmazhatják: biztosíthatnak rejtett távoli elérést (backdoor) egy adott számítógéphez, ellenőrizhetik a billentyűleütéseket, valamint specializálódhatnak jelszavak, banki információk, személyes adatok ellopására – a legtöbb kémprogram ez utóbbi kategóriába esik. De honnan a név, miért pont trójai és miért faló? Ehhez tegyünk egy icipici kerülőt a történelemórák világába. A görögök *Odüsszeusz* ravasz tanácsára építették azt a mondabeli híres, fából készült hatalmas lovat, amelynek belsejében a legbátrabb görög harcosok rejtőztek el. A falovat a csatamezőn hagyták, majd hajóikkal cselesen visszavonulást színleltek. A trójaiak *Kasszandra* és *Laokoón* figyelmeztetése ellenére bevontatták a falovat a városukba, a hatalmas és bevehetetlen falak mögé és örömünneplésbe kezdtek, nehéz boros kupáikat a váratlan győzelemre sokszor emelték és itták ki. És ez lett a vesztük, mert az éjszaka leple alatt a görög harcosok csendesen kimásztak a faló belsejéből, megnyitották a város kapuit és a beáramló görög seregek sok évnyi hiábavaló háborúskodás után végül mégis elfoglalhatták Trója városát – igaz, nem erővel, hanem ésszel.

Történelmi példák: mit tegyünk, ha ki akarnak minket éheztetni?

Ehhez *Fehér M. Jenő* Besenyő őstörténet című munkájából idézünk egy részt. „Értettek a nyílt síkon dúló harc mellett a várostromhoz is, de főleg körülzárással vágták el az erődítményeket a külvilágtól, kiéheztetve a várvédőket. Így történt 995-ben is, amikor kihasználták Belgorod vára környékét és a szokásos türelemjátékkal kiéheztették a lakosságot. Már-már feladták a várat, de egy öreg és ravasz tanácsosnak az az ötlete támadt, hogy pár utcában, a várkapuhoz közel zsúfolják fel minden élelmet, tereljék oda a még megmaradt vágómarhát és látszólag hanyagságból engedjenek beosonni a várba kémeket. Így is történt, s mikor a kémek beljebb is akartak hatolni az üres utcákon, egyszeriben megrohanták őket, de egyben futni is engedték, hogy jelentést tehessenek főnökeiknek. Így aztán [azok] áradoztak az élelmiszerbőség felől. Erre a jelentésre a besenyő had elvonult a vár alól, feladva az ostromot.” Most pedig megnézzük, mi köze mindennek a mai kártevő-terjesztési módszerekhez.

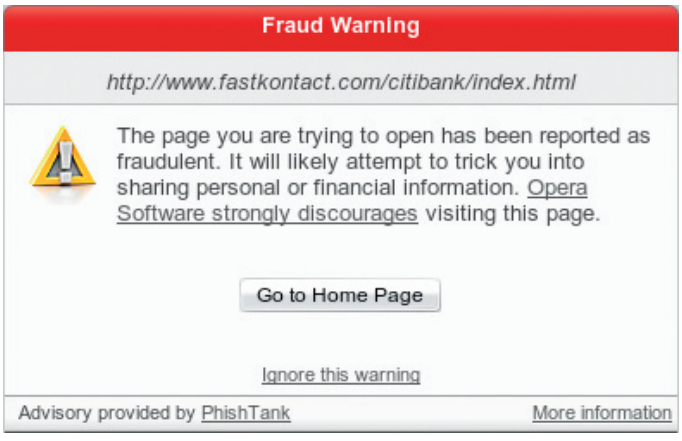


A Bitkom Német Fejlett Technológiai Szövetség felmérése szerint a német internetezők 19 százaléka egyáltalán nem használ vírusirtót a számítógépén, és 54 százalékuknak nincsen telepítve tűzfala. Ha még ehhez hozzávesszük az elhanyagolt biztonsági frissítéseket, akkor látható, hogy ezek az emberek tálcán kínálják gépüket az online bűnözőknek

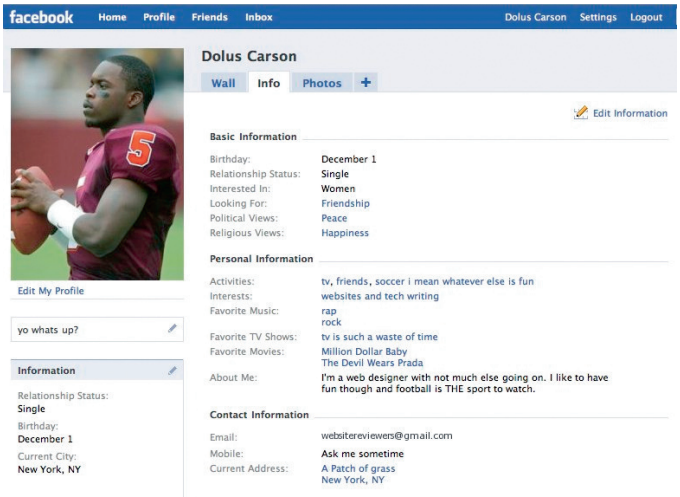
Többet ésszel, mint fűrésszel

Semmi sem állandó, csak a változás maga – szól a Hérakleitosz-idézet nagyon is találóan, rámutatva arra, hogy a kártevők elleni védekezés semmiképpen nem egy kőbevésett statikus szabályrendszer, hanem egy naponta változó, milliónyi trükköt, emberi gyengeséget kihasználó megtévesztés, sok lelemény-nyel és mindig új megnyilvánulási formákkal.

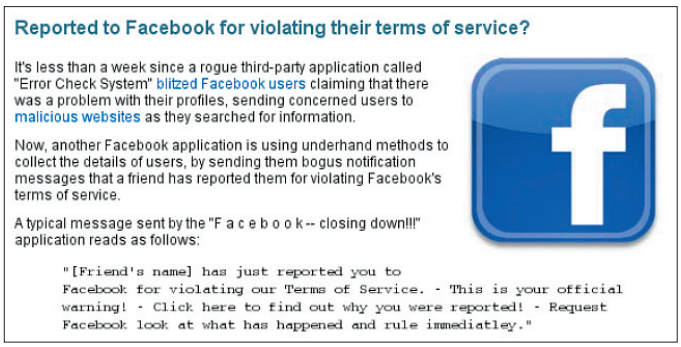
Az örökös harc a biztonsági programokat forgalmazó cégek és a kár-



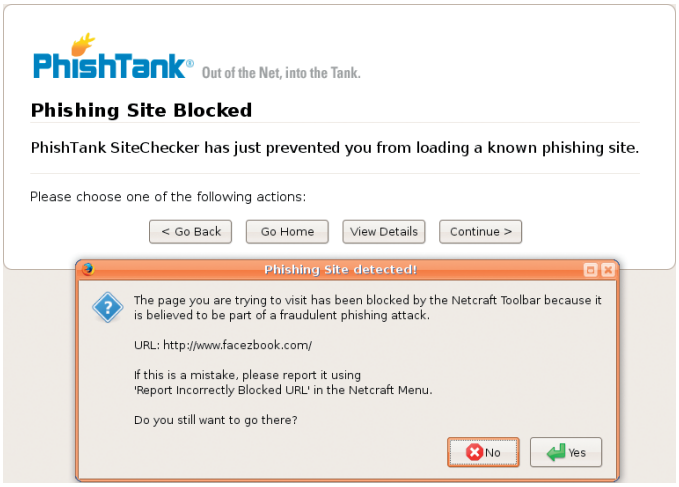
A hamis banki oldalak készítése sem megy ki a divatból, mert mindig akad olyan óvatlan balek, aki hajlandó begépelni az azonosítóit. Már az iskolás kortól el kell(ene) kezdeni a biztonságos netezést, adatkezelést oktatni



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 megjelölő emberek fejében? Az biztos nem, hogy mostantól az új „ismerős” akár beláthat a személyes adatlapjukba is



Itt látszólag a Facebook figyelmeztet minket arra, hogy megsértettük a közösségi oldalon betartandó szabályokat. A valóságban csalók próbálnak minket fertőzött weboldalakra irányítani



Érdemes a PhishTank SiteCheckert (phishtanksitechecker.com) és a Netcraft Toolbart (toolbar.netcraft.com) is telepíteni a Firefox alá. A képen a fentiek sikerrel blokkolják az egy betű eltéréssel rendelkező „facezbook.com" csaló weboldalt. A csalók iparszerűen használják ki az elgépelésből adódó böngésző találatokat is

tevőterjesztők között manapság megszüli az átlagos, védett vonalakat megkerülő megoldásokat, amelyek a találékonyság, a leleményesség megannyi jelét magukon hordozzák. Már számtalan esetben tapasztalhattuk, hogy közösségi portálok vagy azok üzenetei, netán blogbejegyzések kommentjei segítségével próbálnak meg a gépünkre juttatni kártevőket a fejlesztők.

A hatékony védelemhez szükséges, hogy megismerjük az ellenséget – a módszereit, a gondolkodásmódját. A kíváncsiságra („230 halottja van az Európában dúló viharoknak"), a kéjvágyra (*Kurnyikova* meztelen fotói) vagy a pénzsóvárságra (kiemelkedő jövedelem napi egy óra otthoni munkával) épített machinációk minden időben megtalálják a maguk balekjait. Lássunk ezekre pár „jó" példát!

Potya pontok az Xbox Live-re

Egy februári hír szerint veszélybe kerülhetnek az Xbox-tulajdonosok. Akár hitelkártya-adataikat, összegyűjtött pontjaikat és megvásárolt játékaikat is elvesztheti azok az Xbox-felhasználók, akik ingyenes Microsoft-pontok reményében illetéktelen kezekbe adják felhasználónevüket és jelszavukat. A pénzért megvásárolható Microsoft-pontok fizetőeszközként szolgálnak az Xbox-játékkonzolhoz különböző kiegészítő tartalmakat árusító Xbox Live felületen. Ha az internetes bűnözők megszerzik a játékosok belépési adatait, akkor hozzáférhetnek azok személyes és hitelkártya-adataihoz, elkölthetik a Microsoft-pontjaikat, de akár elvehetik az elsősorban presztízsértékű játékospontjaikat (gamerscore) is. Az elkövetők legtöbbször ingyenes pontokat ígérnek a gyanútlan felhasználóknak. Az adathalász weboldalakra irányító üzenetek sokszor játék közben, maguktól a játéktársaktól érkeznek, de a YouTube-on is számos hamis útmutatót találhatunk, ráadásul még a videomegosztó weboldalon található nem egy videó is vírusos fájlt tartalmazó linkekre mutat!

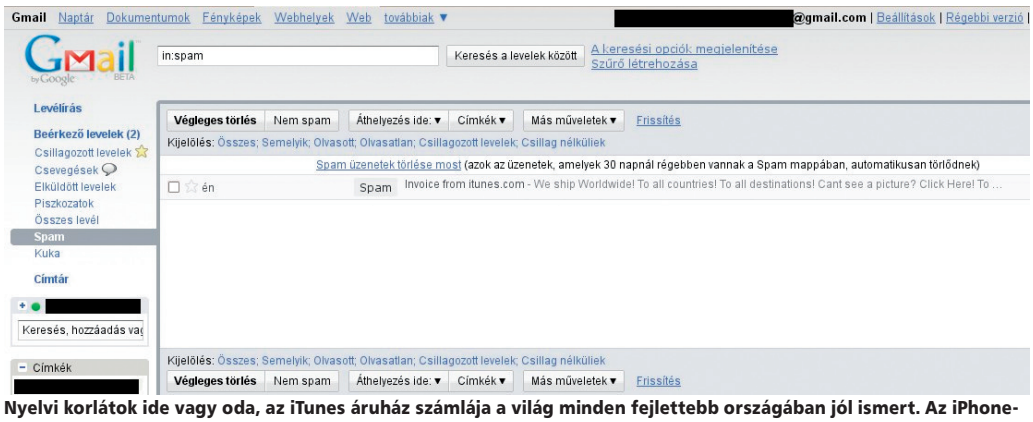
Hamis parkolási büntetőcédulák

Egy másik újonnan felbukkant fortély a parkolással kapcsolatos. Esetünkben az autók szélvédőjére kaptak egy csali értesítő levelet az áldozatok azzal az írással, hogy lefotózták és megbüntették autójukat szabálytalan parkolás miatt, és a mellékelt linken megtekinthetik az inkriminált képet. A büntetőcédulák persze hamisak voltak, a weboldal pedig kártékony szoftvereket próbált telepíteni az áldozatok számítógépére. Azért lássuk be, valóban nagy a kísértés, hogy valaki gondolkodás nélkül ellátogasson a megadott „hivatalos" oldalra.

Megmentsük-e Teréz anyut?

De jut a trükkökből a társkeresőknek is. Ahogy a szegény országokban önálló foglalkozás lett a gazdag turisták autói elé ugrani, aztán pénzbeli kártérítést követelni, miközben persze egy egész falu tanúskodik, hogy „mindent látott", úgy tűnik, az iparszerű házasságszédelgők is sportot űznek a gyanútlan ügyfelek megkopasztásából.

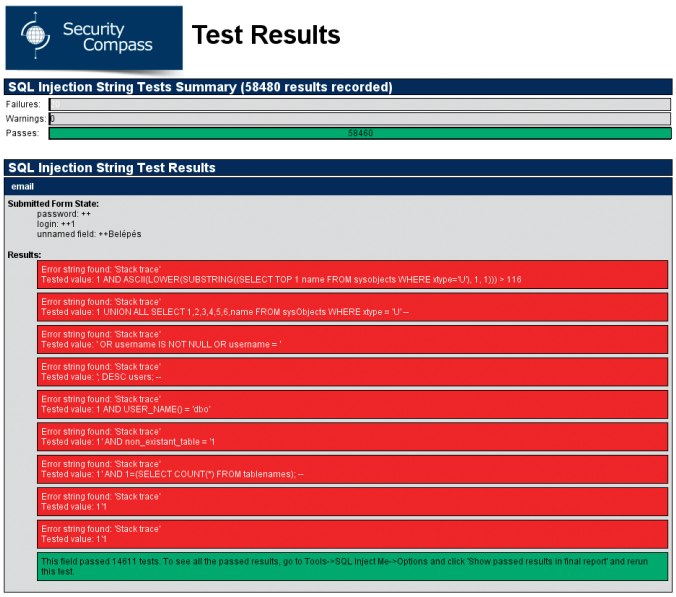
A trükk lényege, hogy az ismerkedés már barátibb szakaszában, amikor az ismerkedők már túl vannak az első levélváltásokon, de még a valódi találkozás előtt állnak, a csaló előáll egy kifogással, hogy valamelyik családtagja váratlanul súlyosan megbetegedett, és pénzzavarában segítséget kérne. Aki bedől az ilyen mesének, vélhetően sosem fogja megtalálni a hercegét fehér lovon. Sokkal valószínűbb, hogy a pénz küldése után bottal ütheti a nyomát a hercegnek és az összegnek egyaránt. A történet külföldön már annyira gyakori, hogy az áldozatok egy külön honlapon osztják meg egymással információikat.



Nyelvi korlátok ide vagy oda, az iTunes áruház számlája a világ minden fejlettebb országában jól ismert. Az iPhone-tulajdonosok rendszeresen megkapják az angol nyelvű számlájukat, de ami ezen a képen szerepel, az már egy hamis levél, és egy „kanadai" gyógyszerészoldalra továbbítja az óvatlanul kattintót

Ugye, mi jó barátok vagyunk?

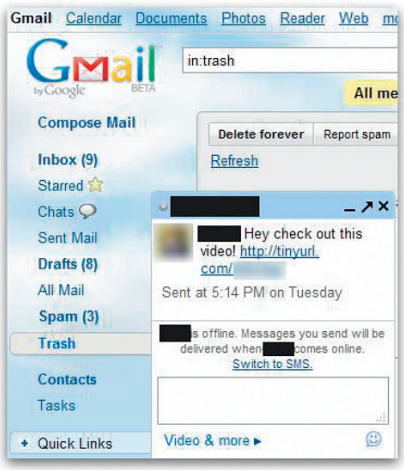
Nem mindenki az, akinek mondja magát – ehhez még Arsène Lupin-rajongónak sem kell lenni, mindenki megtapasztalhatta már. Kísérletező kedvű emberünk egy meglepő eredményű próbát tett az egyik közösségi portálon. Regisztrált a Facebookra – de megtehette volna bárhol máshol is – és összeállított egy kamu adatlapot. Kellett



A támadók már a feltörhető weboldalak felderítésénél is eredményesen támaszkodnak a Google-re. A hibás vagy input-ellenőrzés nélküli dinamikus oldalakat pedig SQL-beillesztéses támadással veszik kezelésbe. Érdemes magunknak is letesztelni az ilyen gyengeségeket, például az SQL Inject Me nevű Firefox-pluginnel (hopp.pcworld.hu/5673)

hozzá egy új e-mail cím, majd jött a hasraütésszerű keresztnév-választás – valami jól csengő, hangzatosra volt szükség – és ezt keresztezte aztán a blogjában használt álnevével, majd máris megszületett *Dolus Carson*. Aztán kell még egy vonzó fotó – esetünkben ez *Marcus Vicket*, egy 183 cm magas, 93 kg-os amerikai profi futballistát ábrázolja, és már lehet is töltögetni a kamu adatlapot. Egy-két véletlenszerűen kiválasztott egyetem, középiskola, klub bejelölése csodát tehet és máris indulhat a „Kit ismerhetek?" című népi játék. Az első harminc perc nehezen akart eltelni, de végül szép részeredménnyel zárult: tíz „barát" megszerzése volt az a pont, ahol megtört a jég. Innentől már könnyebben kaphatunk újabbakat, csak a legelsőt olyan pokoli nehéz megszerezni. Alig négy nap leforgása alatt mintegy száz ismerősre lehetett így szert tenni.

Itt nemcsak arról van szó, hogy valakik tévedésből jelölték meg az adott illetőt ismerősnek, hanem arról, hogy akinek menő barátai vannak, az népszerűbb ember lehet. Az az könnyen akadnak olyanok, akik boldogan vallják barátjuknak a sosem látott, jó kiállású illetőt. Az új barátok aztán már hozzák a „közös ismerősöket" akkor is, ha ez a profil egy, a valóságban nem is létező személyről szól. És persze a népszerű Dolus Carson már láthatja is az ismerősei részletes adatlapját. A statisztikák azt mutatják, hogy az ismerősöktől vagy az ismerősök ismerőseitől érkező levelekre, üzenetekre, linkekre aztán már sokkal könnyebben kattintanak az emberek. Sok magyaráznivaló nincs is azon, miért lehet veszélyes egy ilyen fantom barátság a későbbiekben.



Jó példa, hogy a kártevőre mutató link bárhonnan érkezhet. A Gtalk ablak a ViddyHo videós weboldalt ajánlhatja egy látszólag valódi ismerősünk nevében érkezett üzenettel. A linkre kattintva azonban már töltődik is a kártevő

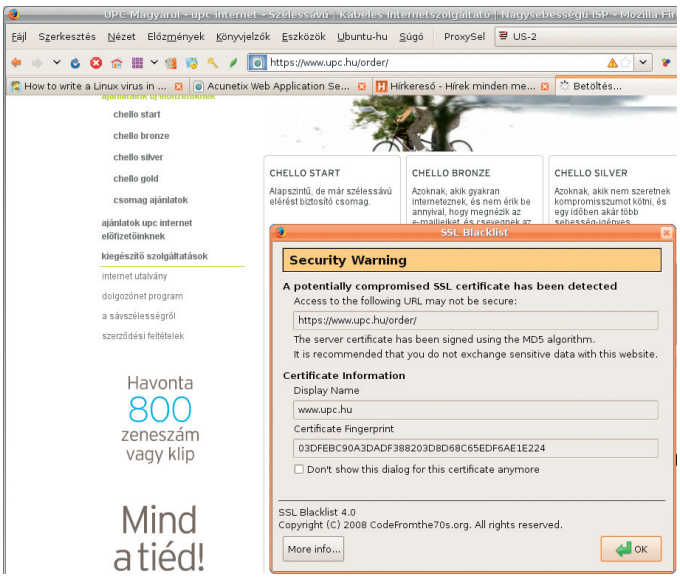
Csillagok háborúja vagy Végtelen történet?

Obi-Wan Kenobi mondta, hogy „Harcolni sokféleképp lehet." Úgy tűnik, minden kártevőterjesztő látta a filmet, mert valóban ontják a trükköket. Megtartják a már felismert, de ennek ellenére működő verziókat is: megy azért a levélmelléklet is, küldik az ünnepi képeslapoknak látszó e-maileket, a klasszikus banki adathalász üzeneteket, de a repertoár egyre bővül, és aki nem figyel oda, nem áldoz időt és pénzt a biztonságáért, az veszteségeket kénytelen elszenvedni. Ahogy az Ösztön (Instinct) című filmben is hallhattuk a „mit veszthetünk" kérdésre adott választ: ártatlanságunkat és naivságunkat, ez az, amit valóban félre kell tenni, ha eredményesen akarunk küzdeni a modern kori fenyegetésekkel. Az internetezés alapvető szabályairól – így például arról, hogy ne adjuk ki felhasználónevünket, bankkártyánk adatait és jelszavunkat ismeretlen oldalakon – még egy jó biztonsági program birtokában sem szabad megfeledkeznünk.

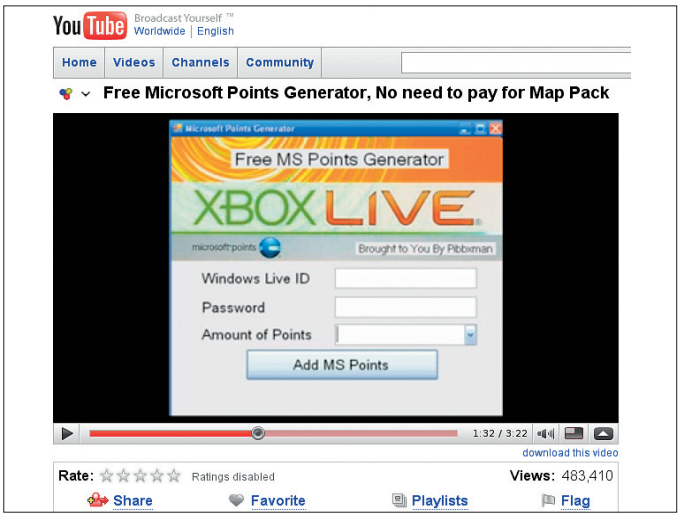
***

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



Az SSL Blacklist (hopp.pcworld.hu/5672) alapból figyelmeztet az olyan gyenge, MD5-lenyomattal rendelkező tanúsítványokra, amelyek a már 2004-ben publikált MD5-ütköztetéssel támadhatóak



Veszélybe kerülhetnek az Xbox-tulajdonosok, ha bedőlnek a pontgyűjtési csalásnak. Akár hitelkártya-adataikat, összegyűjtött pontjaikat és megvásárolt játékaikat is elveszthetik azok a felhasználók, akik ingyenes Microsoft-pontok reményében illetéktelen kezekbe adják felhasználónevüket és jelszavukat

KAPCSOLÓDÓ WEBOLDALAK

A ESET magyar nyelvű víruslexikona: **www.eset.hu/virus**
SSL Blacklist Firefox-kiegészítő: **hopp.pcworld.hu/5672**
SQL Inject Me Firefox-kiegészítő: **hopp.pcworld.hu/5673**
Netcraft Toolbar: **toolbar.netcraft.com**
www.stop-scammers.com
www.phishtank.com