# Hogyan ne veszítsük el a pénzünket online

**Nézzük meg néhány érdekesebb módját annak, miként is veszíthetjük el értékeinket. A csalók ugyanis már nem a bankot akarják kirabolni a neten, hanem tőlünk, ügyfelektől megszerezni adatainkat, amellyel sokkal összetettebben és hosszabb ideig tudnak kárt okozni.**



Az teljesen egyértelmű, hogy el lehet adni az ellopott hitelkártyaszámot vagy banki adatokat, de forintosítható értéke van akár egy netes közösségi játékban magas szintre fejlesztett karakternek is. Kártékony programok halmaza található még ott is, ahol nem is gondolnánk. Manapság már nem feltétlenül kell megnyitnunk egy e-mail csatolmányát ahhoz, hogy megfertőződjön a számítógépünk, és a települt kártékony program összegyűjtse róla a használható adatokat. A gyenge biztonsággal felépített honlapokat feltörve a csalók olyan kódot ágyaznak a weboldalra, amit a meglátogatásakor akár automatikusan lefuttat a böngészőnk. Lehet, hogy épp teáskannákat nézegetünk tehát a turai népi kézműves egyesület honlapján, és közben néhány azonosítónk és jelszavunk is távozik a gépről. Persze a csalók ott szeretnek próbálkozni, ahol több potenciális célpont található. Napjainkban a fő célpontok a közösségi oldalak, az adathalász kísérletek leginkább ide összpontosulnak.

Amit mi tehetünk a biztonságunk érdekében, hogy használjuk és frissítjük a vírusirtót, tűzfalat, telepítjük a böngészőhöz elérhető frissítéseket. A közösségi oldalakon a lehető legkevesebb adatot adjuk meg magunkról, és körültekintően használjuk/telepítjük az alkalmazásokat, bővítjük ismerőseink körét. Napjainkban a bankok biztonságos megoldásokat dolgoznak ki azért, hogy a pénzünk online is biztonságban legyen. Ki férhet hozzá manapság a webbankjához sms azonosítás nélkül? A legtöbb bank használja ezt a technológiát, ami azonban kijátszható. Az ún. *középreállásos támadásnak* (man-in-the-middle attack) hús-vér szereplője is van. A trükk egy sima adathalász oldalon indul, a megtévesztett felhasználó elhiszi, hogy be kell lépjen a webbankjába karbantartás miatt. Az ő képernyőjén ott virít a weboldal, melyet a bankjáénak hisz, de valójában csak külsőre hasonlít. A csaló pedig valóban az áldozat bankjának weboldalát meglátogatva készen áll a pénzszerzésre. Az áldozat megadja az adatait és a belépésre kattint. Az oldal töltődik, töltődik... A csalónál megjelennek az adatok, melyeket beír a valódi weboldalra és elkezdi a bejelentkezést. Az áldozat megkapja a hitelesítő kódot sms-ben, amit beír a (csalónak) megfelelő helyre, majd megkapja az üzenetet egy bejelentkezési hibáról és kérést, hogy később próbálkozzon. Később már csak a pénze visszaszerzésével kapcsolatban próbálkozhat a bankjánál. A csaló belép az online felületre, ahonnan az aktuális limitnek megfelelő összeget el tudja távolítani. A bankok számára a fő fegyver a tájékoztatás mellett, hogy a lehető leghamarabb elérjék a csaló weboldal leállítását. Ezeket az oldalakat jellemzően egy feltört weboldalon helyezik el. Lehet, hogy a lacikonyha.hu-t böngészve nem is sejtjük, hogy a lacikonyha.hu/bankofmalaysia-my/loginaccount.html oldalon lelkes károsultjelöltek tehetik kockára a bevételeiket. De ugyanígy egy japán kiszolgálón ráakadhatunk az OTP oldalára is. A hellokitty.jp/otpbank-hu/index.html-nél ha már véletlenül megnyitottuk, a cím eleje lebuktathatja a csalót. Észrevesszük a turpisságot és elküldjük a banknak az információt. A bank több helyről is értesül a kísérletről, és az óra elkezd ketyegni. Ha a weboldal elérhetetlen, nem járhat pórul senki. Ehhez meg kell tudni, hol van elhelyezve a weboldal és megkeresni a szolgáltatót a leállítás kérésével. Sajnos nem lehetünk biztosak benne, hogy mindenki beszél angolul, ezért a hatékonyságot segíti az adott ország internetbiztonsági incidenskezelő csoportjának a megkeresése, ha működik ilyen. A szolgáltatók megszüntetik az elérhetőséget, aztán felszólítják ügyfeleiket a hiányosságok rendbetételére, ha ugyanis nem vizsgálják meg egy fertőzés

**A tavalyi év harmadik negyedévében a fertőzött weboldalak száma a világon meghaladta az 1,2 milliót, ami a duplája az előző év hasonló időszakában tapasztaltnak.**

okát és nem foltozzák be a lyukakat, akkor az újra bekövetkezhet.

Nem kell weboldalakat fertőzni bonyolult programok írásával, ha valahogy elérik, hogy a pénzünket vagy értékeinket önként és dalolva adjuk át. A nigériai csalásokat talán már az is ismeri, akinek még nem volt e-mail címe sosem. A módszer egyszerű, vagy a bedöntött nigériai vagy ghánai miniszter mentené a pénzét a bankszámlánkra, ha előtte mi is csepegtetünk neki, vagy az express.hu-n hirdetett fényképezőnket venné meg egy angol professzor a Nigériában tanuló kisfiának. Utóbbinál ugye a vételárat és a postaköltséget egy kamudokumentummal letétbe helyezettnek mutatják és várják, hogy elküldjük az árut. Nem is erről a remélhetőleg mindenki által ismert csalási formáról írnék most, hanem arról, hogy ugyan sovány vigaszt nyújtva a károsultaknak, de megmosolyogtatva a többieket, tevékenykednek a csalók szívatói, a scam baiterek. Ők a csalók módszereivel csalják lépre áldozataikat. Találkozókat beszélnek meg velük

Jó tanács: az okostelefon egy számítógép, ugyanazok a veszélyforrások, mintha az asztali számítógépünket vagy a laptopunkat használnánk.

veszélyes helyekre vagy olyan fényképek készítését kérik tőlük, amelyen megalázó módon szerepeltetik őket. Legtöbbször valamilyen szöveget íratnak fel velük, amivel aztán fotózkodniuk kell. A szórakozáson kívül így az idejüket, energiájukat is lekötik, amelyet így haszontalanul töltenek el. Angolul tudók a 419eater.com weboldalon találhatnak infromációkat (és persze képeket a rászedettekről) a csoportról.

**gss**

Az interneten a csalók 2009-ben közel 560 millió dollárt szereztek meg áldozataiktól.

*A következő számban:*
*Górcső alatt a facebook!*