Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadványban...

- **Személyes biztonság**
- **Számítógép és felhasználói fiók biztonsága**
- **Tanácsok szülőknek**

Internetes játékok és biztonság

Áttekintés

Az internetes játékok a szórakozás egyik népszerű formája, azonban ezeknek is megvan a saját kockázatuk. Az OUCH! ehavi hírlevelében arról lesz szó, hogyan védhetjük meg magunkat és családunkat, ha internetes játékokat használunk.

A szerzőről

Jake Williams a Rendition Infosec alapítója és vezető tanácsadója, minősített SANS oktató, és számos SANS kurzus társszerzője. A Twitter-en **@MalwareJake** néven található meg, illetve saját blogot vezet a **malwarejake.blogspot.com**-on.

Személyes biztonság

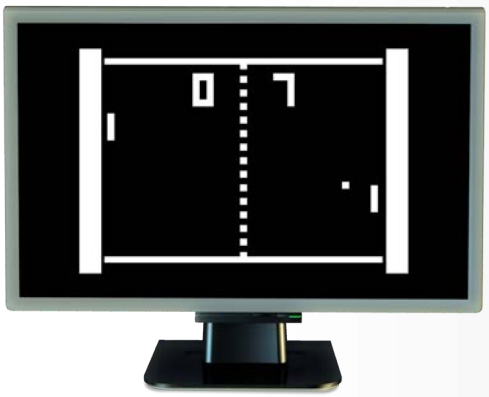
Az teszi igazán vonzóvá az internetes játékokat, hogy a világ minden részéről származó emberekkel tartjuk a kapcsolatot és játszhatunk együtt velük. Általában viszont azt sem tudjuk, hogy valójában kikkel játszunk együtt. Bár az internetes játékosok túlnyomó többsége egyszerűen csak kikapcsolódásra vágyik, azonban vannak köztük rosszindulatú emberek is. Az alábbi tanácsok abban segíthetnek, hogy megelőzzük a bajt:

- Legyünk óvatosak az olyan üzentekkel, amelyekben hivatkozás található, vagy amiben arra kérnek bennünket, hogy töltsünk le egy állományt. Ugyanúgy, mint az adathalász támadásoknál, a bűnözők megpróbálnak átverni bennünket, esetleg káros szoftverrel akarják megfertőzni a számítógépünket. Ha egy üzenet túl gyanúsnak, sürgetőnek vagy túl jónak tűnik, akkor gyanakodjunk, hogy igazából átverés lehet.
- Sok internetes játéknak van saját virtuális piactere, ahol adni-venni, cserélni lehet dolgokat, vagy akár valódi pénzért lehet venni játékbeli tárgyakat. Pont úgy, mint a való életben, itt is lehetnek csalók, akik megpróbálják kicsalni vagy csak simán ellopni a pénzünket.
- Legyünk óvatosak az olyan tranzakciókkal, ahol valódi pénzt adunk virtuális tárgyakért (vagy éppen fordítva). Az ilyen tranzakciókat csak a játék hivatalos piacterén hajtsunk végre, és ott is csak a jó „hírnévvel” rendelkező játékosokkal.
- Minél kevesebb információt adjunk ki saját magunkról vagy a családunkról, és soha ne adjunk meg olyan személyes információkat, mint a jelszavunk vagy éppen a lakcímünk.
- Számos weboldal (pl. online bankok) használnak biztonsági kérdést arra, hogy bejelentkezéskor meggyőződjenek a felhasználó valódiságáról. Amennyiben összebarátkozunk valakivel egy internetes játékban, az könnyen szerezhet olyan információkat, amelyeket fel tud használni egy ellenünk irányuló támadásban. Ne felejtsük el, hogy egyetlen játékban sem vagyunk kötelesek válaszolni a magánéletünkre vonatkozó kérdésekre.

Internetes játékok és biztonság

Számítógép és felhasználói fiók biztonsága

A következő lépés, hogy biztonságossá tegyük a játékra használt számítógépünket, mivel a bűnözők megpróbálhatják megszerezni a rendszerünk feletti irányítást, vagy hozzáférni a játékban használt felhasználói fiókhoz.



Az internetes játékok biztonságának alapja az erős jelszó, a biztonságos számítógép, valamint ha idegenekkel állunk szóba, akkor a józan eszünk használata.

- Használjunk erős jelszót a számítógéphez és a játékok felhasználói fiókjához, így a bűnözők nem tudják egyszerűen kitalálni a jelszavunkat, hogy átvegyék azok irányítását. Ha a játék lehetőséget ad a kétlépcsős bejelentkezésre, akkor használjuk azt. Ne használjuk ugyanazt a jelszót különböző játékokhoz, így ha az egyikhez tartozó jelszót megszerzi valaki, akkor a többi még mindig biztonságban van.
- Mindig telepítsük a játékra használt operációs rendszer, illetve magának a játék szoftvernek a legújabb frissítéseit. A játékok ebből a szempontból nem különböznek más szoftverektől, és a régebbi verziókban lévő hibákat a bűnözők felhasználhatják arra, hogy feltörjék a számítógépünket. Azzal, hogy mindig naprakészen tartjuk a rendszerünk összes szoftverét, kiküszöböljük annak a kockázatát, hogy a bűnözők kihasználják a sérülékenységeket.
- Folyamatosan legyen bekapcsolva a naprakész antivírus szoftverünk.
- Mindig megbízható helyről töltsük le a játékokat. Csak a hivatalos gyártó (kiadó) vagy más ismert, megbízható weboldalról töltsünk le játékokat, mert gyakran előfordul, hogy a kiberbűnözők hamis vagy káros szoftverrel fertőzött játékokat terjesztenek. Amennyiben egy ilyet telepítünk a gépünkre, azzal szabad utat engedünk a bűnözőknek, akik átvehetik a rendszerünk irányítását.
- Egy játék körül létrejövő közösség gyakran ír saját kiegészítő programokat (add-on), vagy készít új tartalmakat az alapjátékhoz. A bűnözők gyakran az ilyen kiegészítőket is megfertőzik káros szoftverekkel, amit aztán nagyon nehezen ismernek csak fel az antivírus programok. Az ilyen kiegészítő tartalmakat és programokat is megbízható forrásból töltsünk le. Ha egy kiegészítő tartalom azt kéri, hogy kapcsoljuk ki az antivírus szoftvert, vagy módosítsunk a tűzfalon, akkor azt semmi esetre sem szabad megtennünk.
- Külön underground közösségek jöttek létre azért, hogy csaló (cheating) programokat készítsenek. Azon kívül, hogy a csalás etikátlan dolog, gyakran nagyon fejlett káros szoftvereket (root-kit) tartalmaznak. Soha ne telepítsünk és használjunk csaló programokat.
- Látogassuk meg az általunk használt játékok weboldalát, ahol gyakran külön fejezetet szentelnek a biztonsági beállításoknak és tanácsoknak, amiket érdemes megfogadni.
- Legalább olyan óvatosan járjunk el akkor is, ha a mobiltelefonunkon játszunk, mintha az otthoni számítógépünkön tennénk ugyanezt. A kiberbűnözőknek az egyre fejlettebb eszközök is vonzóbb célponttá válnak.

Internetes játékok és biztonság

Tanácsok szülőknek

Szülőként győződjünk meg arról, hogy a gyermekünk követi a fenti tanácsokat (fiatalabb gyerekek esetén saját magunk hajtsuk végre ezeket), valamint beszélgessünk el velük a veszélyekről. A figyelemfelhívás és a nyílt párbeszéd a leghatékonyabb módszer arra, hogy megvédjük őket a veszélyektől. A legjobb módszer az, ha leülünk velük, és megkérjük őket, hogy mutassák be a játékot, hogy néz ki, hogy működik, és akár mi magunk is beszállhatunk velük játszani. Ezen kívül fontos, hogy elmagyarázzuk nekik, hogy különféle emberekkel találkozhatnak a játékban. Elég gyakori, hogy a gyerekek a közösségi életük nagy részét internetes játékokon keresztül élik meg. Azzal, hogy beszélünk velük (és ők beszélgetnek velünk) ezekről a dolgokról, hatékonyabban meg tudjuk őket védeni, mint bármilyen technológia.

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a http://www.securingthehuman.org weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További információ a http://www.nisz.hu oldalon olvasható.

Hivatkozások

Pszichológiai manipuláció:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_hu.pdf
Adathalász támadások:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_hu.pdf
Jelszavak:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_hu.pdf
Mi Mi az a vírusvédelem?:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201412_hu.pdf
Biztonságos internetezés:	http://www.biztonsagosinternet.hu

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Fordította: Birkás Bence, Árvai Gábor