OUCH! 2022. június

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Online játék biztonságosan

Az online játékokat az teszi annyira szórakoztatóvá, hogy a világ bármely pontjáról játszhatunk és kommunikálhatunk másokkal, még ha a legtöbb esetben nem is ismerjük azokat, akikkel játszunk. Az emberek túlnyomó többsége az interneten ugyanúgy szórakozni szeretne, mint mi, azonban sajnos vannak, akik kárt akarnak okozni.

Védjük adatainkat!

Az online játékokkal kapcsolatos legnagyobb kockázatot nem maga a technológia jelenti, hanem az idegenekkel folytatott interakció.

- Legyünk óvatosak minden olyan üzenettel kapcsolatban, amelyben valamilyen művelet végrehajtására kérnek bennünket, például, hogy kattintsunk egy hivatkozásra, vagy töltsünk le egy fájlt! A támadók legtöbbször játékon belüli üzenetekkel vagy adathalász e-mailekkel próbálják meg rávenni az áldozatot egy olyan műveletre, amellyel megfertőzhetik a számítógépét, ellophatják személyazonosságát vagy játékfiókjait. Ha egy üzenet furcsának, sürgetőnek vagy túl szépnek tűnik, ahhoz hogy igaz legyen, gyanakodjunk arra, hogy egy támadásról van szó!
- Sok online játéknak saját online piactere van, ahol a játékos virtuális javakat vásárolhat, vagy ezekkel kereskedhet. Éppúgy, mint a való világban, ezeken a virtuális piactereken is léteznek csalók, akik megpróbálják átverni a játékosokat, és ellopni a pénzüket vagy virtuális valutájukat. Csak olyan emberektől vásároljunk, akik leellenőrizhetőek és megbízhatóak!
- Használjunk erős, egyedi jelszót minden játékfiókunkhoz! Így a támadók nem tudják egyszerűen kitalálni jelszavainkat, és átvenni az irányítást fiókjaink felett. Ha adott a lehetőség a kétlépcsős azonosításra, vegyük igénybe! Problémát jelent az összes jelszó észben tartása? Használjunk jelszókezelőt!

A számítógép biztosítása

A támadók megpróbálhatják feltörni a számítógépet vagy eszközt, amelyen játszunk, ezért lépéseket kell tennünk annak védelme érdekében.

- Mindig frissítsük eszközeinket az operációs rendszer és a játékszoftver vagy mobilalkalmazás legújabb verziójára! Az elavult szoftverek ismert sérülékenységekkel rendelkezhetnek, amelyeket a támadók kihasználhatnak eszközeink feltörésére. Ha lehetséges, engedélyezzük az automatikus frissítést! Azáltal, hogy eszközeinket és játékalkalmazásainkat naprakészen tartjuk, kiküszöbölhetjük a legtöbb ismert sebezhetőséget.
- Csak megbízható webhelyekről töltsünk le játékszoftvereket és játékkiegészítő csomagokat! A támadók gyakran készítenek hamis vagy fertőzött verziókat a programokról, amiket aztán a saját szervereikről terjesztenek. Ezenkívül, amennyiben egy játék vagy kiegészítő bármilyen biztonsági eszköz leállítását vagy tiltását kéri, ne használjuk az adott programot!

- A videójátékokban való csalás (cheatelés) az underground fórumok egyik legnépszerűbb témája. Jó ha tudjuk, hogy amellett, hogy a cheatelés etikátlan, sok csaló program rosszindulatú kódokat is tartalmaz, amely megfertőzhetik az eszközeinket. Soha ne telepítsünk vagy használjunk semmilyen csaló szoftvert vagy webhelyet!
- Mindig ellenőrizzük az online játékszoftver webhelyét! Sok játékoldalon találhatunk útmutatót arról, hogy hogyan védhetjük meg rendszerünket.

Szülőknek, gondviselőknek

Az oktatás és a gyermekekkel folytatott nyílt párbeszéd a leghatékonyabb lépés, amelyet a védelmükben megtehetünk. Jó megközelítés az, ha megkérjük őket, mutassák meg, hogyan működnek a játékaik, így képet formálhatunk arról, hogy manapság milyen a videójátékok világa. Akár játszhatunk is együtt. Ami azonban lényeges, kérjük meg őket, írják le kik azok, akikkel az online térben találkoznak. Ma már a gyermekek társasági életének jelentős része az online játékok világában zajlik. A legkönnyebben akkor fedhetjük fel az esetleges problémákat, és védhetjük meg gyermekeinket, ha beszélünk velük, és meghallgatjuk őket. Ez bármely technológiai megoldásnál (például szülői szoftver) hatékonyabb. Néhány további lépés, amit megtehetünk:

- Győződjünk meg arról, hogy a gyermekünk által játszott játék az életkorának megfelelő!
- Korlátozzuk a gyermekünk által online megosztható információk mennyiségét! Például soha ne osszuk meg másokkal jelszavukat, életkorukat, telefonszámukat vagy otthoni címüket!
- Jó, ha a játékra használt eszközt olyan nyitott területen helyezzük el, ahol mi is szemmel tarthatjuk. Figyeljünk oda arra, hogy a kisebb gyerekek ne játszhassanak a szobájukban vagy például késő este!
- A zaklatás, trágár beszéd vagy más antiszociális viselkedés problémát jelenthet. Vegyük észre, ha gyermekünk egy játék után idegesnek tűnik, mert ez jelezheti, ha zaklatják az interneten. Ha kiderül, hogy valóban zaklatják a gyermeket, jelezzük ezt a játék webhelyén, és csak az általunk is ismert barátaival engedjük online játszani!
- Tudjuk meg, hogy gyermek játékai támogatják-e az alkalmazáson belüli vásárlásokat, és milyen szülői kontrollt biztosítanak!

A szerzőről

Charlie Goldner a CyberNV alapítója és SANS oktató. Aktív a LinkedIn-en, fő feladata a kormányzati szervek támogatása. Ő maga is tapasztalt játékos, az évek során sok órát töltött játékokal PC-n és konzolokon.

Források

Pszichológiai manipulációs támadások:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltc531b800ae30add6/6048fee908636f3d7749ce3f/OUCH!_Nov_2020_-_Social_Engineering_v.3-Hungarian.pdf
Egy egyszerű lépés a felhasználói fiókunk biztonságáért:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltd7ca6894e2f888b9/6137f5d4fbf2f03cb2533d9f/ouch!_september_2021_one_simple_step_to_securing_your_accounts_Hungarian.pdf
Jelszókezelők:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt9835f222e67b748e/604a692c982f2a0bdaf5dea1/202004-OUCH-Hungarian.pdf
Online biztonság gyerekeknek:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltf8688a7b5eb9b302/6047fb66a8c6585cda24cc4c/September_2020_-_Securing_Kids_Online_(Chris_Pizor)_v5-Hungarian.pdf

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)