Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

- **A tablet biztonsága**
- **Hogyan maradjunk továbbra is biztonságban?**

Az új tablet és a biztonság

Áttekintés

Gratulálunk az új tablet-hez. Ez az eszköz hatékony és kényelmes módját biztosítja, hogy kapcsolatba lépjünk másokkal, online boltokban vásároljunk, filmeket nézzünk, játsszunk, vagy millió más tevékenységet végezzünk. Mivel a tablet-ek egyre fontosabb szerepet töltenek be az életünkben –akár még a számítógépet is helyettesíthetik – tisztában kell lennünk pár olyan dologgal, amelyek segíthetnek bennünket abban, hogy mind a tablet, mind a rajta tárolt információk biztonságban legyenek.

A szerzőről

Lori Rosenberg hatalmas tapasztalattal rendelkezik információ biztonsági oktatóanyagok készítésében és oktatásában mind céges alkalmazottak, mind pedig ilyen eszközök vásárlói számára, és szenvedélyesen keresi az új lehetőségeket, hogy tudását megossza másokkal. A Twitter-en **@InfoSecLori** néven találhatjuk meg.

A tablet biztonsága

Talán meglepő lehet, de a tablet-re nem a hacker-ek jelentik a legnagyobb veszélyt, hanem mi, a felhasználók. Gyakrabban veszítjük el, hagyjuk ott valahol, vagy éppen lopják el tőlünk, minthogy egy kiberbűnöző távolról feltörje. A legelső dolog, amit meg kell tennünk, az az automatikus képernyőzár bekapcsolása. Ez azt jelenti, hogy ha használni akarjuk az eszközt, akkor be kell írnunk egy jelszót, az ujjunkat egy előre beállított minta szerint kell végighúzni a képernyőn, vagy akár magát az ujjlenyomatunkra is szükség lehet a zárolás feloldásához. Ez biztosítja azt, hogy ha elveszítjük vagy ellopják a tablet-et, akkor senki ne tudjon hozzáférni a rajta tárolt információkhoz, alkalmazásokhoz, stb. Miután bekapcsoltuk az automatikus képernyőzárat, az alábbi tanácsok további segítséget jelenthetnek a biztonság növelése érdekében:

1. Telepítsünk és/vagy engedélyezzünk olyan szoftvert a tablet-re, amely lehetővé teszi a távoli nyomkövetést! Ha elveszítjük, ellopják az eszközt, akkor ennek a szoftvernek és az Internet segítségével meg lehet határozni a pontos helyét, de legrosszabb esetben akár távolról törölhetjük is a rajta található adatokat.
2. Frissítsük az eszköz szoftverét, és kapcsoljuk be az automatikus frissítést is! Ezzel a lépéssel gondoskodhatunk arról, hogy mindig a legfrissebb, legbiztonságosabb operációs rendszert használjuk. A bűnözők folyamatosan keresik a szoftverekben lévő, kihasználható hibákat, a gyártók pedig folyamatosan készítik ezeknek a feltárt hibáknak javításait. Azzal, hogy mindig a legfrissebb operációs rendszert és alkalmazásokat használjuk, megnehezítjük a kiberbűnözők dolgát, és sokkal nehezebben tudják feltörni a tablet-ünket.
3. Fokozott figyelmet fordítsunk a tablet üzembe helyezésekor az adatvédelmi beállításokra. Az egyik legnagyobb veszélyt

Az új tablet és a biztonság

az jelenti, hogy mások képesek lehetnek nyomon követni bennünket, így mindig tudhatják, hogy éppen hol tartózkodunk. Érdemes tiltani azt, hogy minden hozzáférjen ehhez a funkcióhoz, és csak annak az alkalmazásnak engedélyezni, ami esetén valóban úgy érezzük, hogy szükséges lehet. Néhány alkalmazásnak valóban szüksége lehet erre a funkcióra (pl. térképszoftverek, közeli éttermek keresésére való app-ok, stb.), de a legtöbbnek valójában nincs szüksége valós idejű nyomkövetési adatokra.

4. A legtöbb tablet és az alkalmazások egyaránt a felhőben (cloud) tárolják az adatainkat. Emiatt nagyon fontos, hogy tisztában legyünk azzal, hol vannak az adataink, és milyen módon vannak biztosítva. Nyilván egyikünk sem örülne annak, ha a privát képeinket az egész internet láthatná, ráadásul úgy, hogy pontosan tudják, mikor és hol készültek. Ezért javasoljuk, hogy alapértelmezetten tiltsunk le minden felhős megosztást, és csak akkor engedélyezzük, ha valóban meg akarunk osztani valamit az ismerőseinkkel.

A biztonságos tablet használat alapjai a képernyő zárolás engedélyezése, a biztonsági beállítások felülvizsgálata, és az eszköz rendszeres frissítése.

5. A tablet-en lévő alkalmazásokban tárolt adatok folyamatosan szinkronizálódnak az egyéb eszközeinken (laptop, okostelefon) lévőkkel. A szinkronizáció egy nagyszerű lehetőség, de kezeljük óvatosan, és gondoljuk meg alaposan, hogy milyen alkalmazásoknak engedjük meg a használatát. Amennyiben be van kapcsolva a szinkronizálás, ne lepődjünk meg, ha a munkahelyi böngészőnkben pont ugyanazok a weboldalak jelennek meg, amiket a tablet-en is megnyitottunk.

Hogyan maradjunk továbbra is biztonságban?

Miután gondoskodtunk a tablet megfelelő biztonsági beállításairól, szeretnénk, ha ez a jövőben is így maradna. Az alábbi tanácsok segítenek abban, hogy ez hosszú távon is így legyen:

- Soha ne kerüljük meg az eszköz alap biztonsági beállításait, mivel ezek számos olyan biztonsági rést iktatnak ki, amelyekkel sokkal sérülékenyebb lenne a tabletünk.
- Csak olyan alkalmazást töltsünk le, amire valóban szükségünk van, és azt is csak biztonságos forrásból! Az Apple pl. minden alkalmazást bevizsgál, mielőtt elérhetővé teszik. Az Android-os eszközökre csak a Google alkalmazásboltját használjuk, az Amazon tablet-ek esetén pedig az Amazon App Store-t. Ha más weboldalról töltünk le alkalmazásokat, akkor nem lehetünk abban biztosak, hogy azokat megfelelően átvilágították, és lehet, hogy káros szoftverrel fertőzöttek. Végezetül pedig, ha már nem használjuk az alkalmazást, akkor töröljük le az eszközről, bárhonnan is szereztük be azt.

Az új tablet és a biztonság

- Amikor új alkalmazást telepítünk, mindig nézzük át az adatvédelmi beállításokat, pontosan úgy, ahogy a készülék megvásárlása utáni első konfigurálás esetén is! Legyünk körültekintőek abban, hogy mihez engedünk hozzáférést az újonnan telepített programok számára! Például gondoljunk csak bele, hogy a frissen letöltött alkalmazásnak valóban szüksége lehet a barátaink telefonszámára és email címére? Ha kényelmetlennek érezzük az alkalmazás ilyen és hasonló adatok iránti kérelmét, akkor inkább keressünk más megoldást! Ezen túl pedig rendszeresen ellenőrizzük a már megadott engedélyeket, hogy időközben nem változtak-e meg!

A tablet-ünk egy rendkívül hasznos eszköz lehet, amit használni és élvezni szeretnénk. A fenti tanácsok észben tartásával hosszú időre gondoskodhatunk az eszköz biztonságáról.

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

Mobil alkalmazások biztonságos használata:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201501_hu.pdf
Jelmondatok:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_hu.pdf
A felhő biztonságos használata:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201409_hu.pdf
Mielőtt megválunk a régi mobilunktól:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201406_hu.pdf
SANS napi biztonsági tipp (angolul):	https://www.sans.org/tip_of_the_day.php

OUCH! a SANS Securing The Human program által közzétett hírlevél, amelyre Creative Commons BY-NC-ND 4.0 licensz feltételei vonatkoznak. A hírlevél szabadon terjeszthető vagy felhasználható tudatosító programban, addig amíg az nem kerül módosításra. A fordításért vagy további információért kérjük írjon az ouch@securingthehuman.org címre.

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

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus