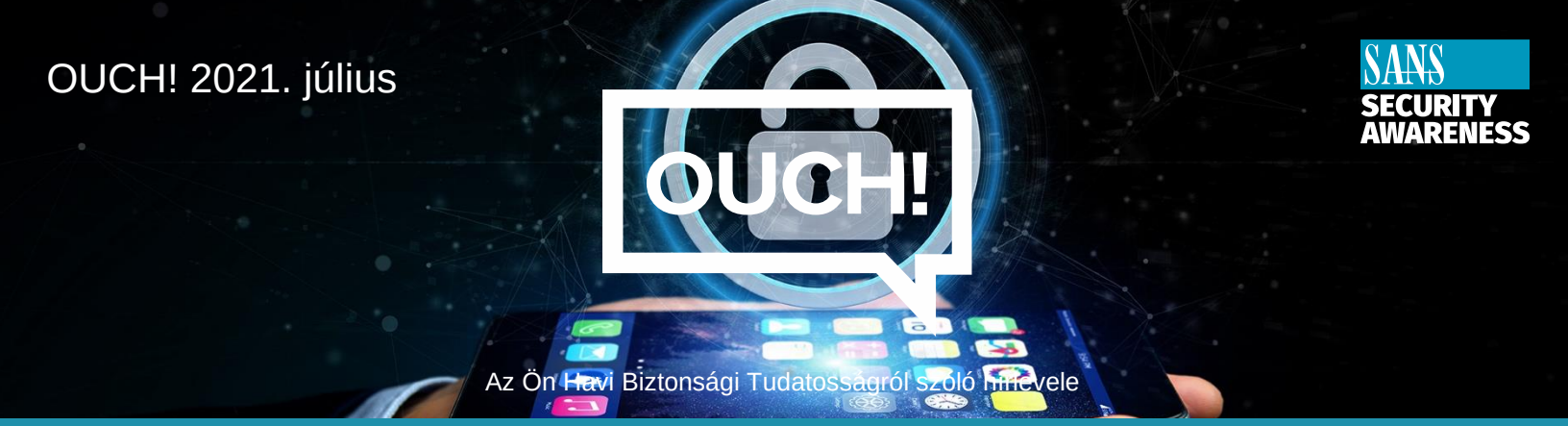

Mobileszközeink biztonságos használata

Áttekintés

Mobileszközeink elképesztően egyszerűvé teszik a barátokkal való kommunikálást, vagy – sok egyéb tevékenység mellett – a vásárlást, online bankolást, és a szórakozást. Mivel ezek az eszközök mindennapi életünk fontos részét képezik, alapvető fontosságú, hogy biztonságossá tegyük őket.

Így tegyük biztonságossá eszközeinket

Meglepő lehet, de jó, ha tudjuk, hogy eszközeink biztonságára nézve nem is a kiberbűnözők, hanem mi magunk jelentjük a legnagyobb kockázatot. Ugyanis sokkal nagyobb a valószínűsége annak, hogy elveszítjük a készülékünket, mint hogy azt valaki meghekkelje. A legfontosabb védelmi intézkedés, hogy bekapcsoljuk az automatikus képernyőzárat. Ez azt jelenti, hogy amikor használni szeretnénk a készüléket, fel kell oldanunk a képernyő zárolását jelszó megadásával vagy ujjlenyomat, esetleg arcfelismerés segítségével. Ezáltal nagyban megnehezíthetjük illetéktelenek számára, hogy hozzáférjenek az eszközünkön tárolt érzékeny adatainkhoz, amennyiben elveszítenénk a készüléket. Ráadásul a legtöbb mobileszköz esetében a képernyő zárolása egyben titkosítja is az eszköz tartalmát, ami egy további adatvédelmi funkciót jelent.

A következőkben további védelmi tippeket mutatunk be:

1. **Frissítés**: Engedélyezzük az automatikus frissítéseket, így mindig a legújabb verziójú szoftverek (operációs rendszer és alkalmazások) futnak majd a készülékeinken. A támadók folyamatosan új szoftversebezhetőségek után kutatnak, a programok fejlesztői pedig biztonsági frissítések segítségével igyekeznek kijavítani ezeket. Eszközeink naprakészen tartása jelentős védelmet biztosít az ellen, hogy valaki feltörje őket. Amikor új androidos eszközt vásárolunk, ellenőrizzük, hogy a készülék gyártója meddig nyújt biztonsági támogatást az adott készülékhez. Az Apple iOS eszközöket maga a cég frissíti, míg Android rendszer esetén a készülékgyártók végzik el a frissítést, azonban nem minden gyártó aktív a frissítések kiadását illetően. Ha régebbi készülékkel rendelkezünk**, amit már nem lehet frissíteni, fontoljuk meg, hogy vásárolunk egy újat, amihez jár szoftveres támogatás.**

2. **Nyomon követés**: Telepítsünk megbízható szoftvereket, hogy eszközünk helyzetét az interneten keresztül, távolról nyomon tudjuk követni, vagy ha rendelkezésre áll ilyen beépített funkció, aktiváljuk azt. Ennek segítségével távolról kapcsolódhatunk eszközünkhöz, hogy meghatározzuk a készülék földrajzi helyzetét, amennyiben azt elveszítettük vagy ellopták tőlünk. Emellett, ha szükséges, távolról törölhetjük is az adatainkat.

3. **Megbízható mobilalkalmazások**: Csak azokat az appokat telepítsük, amire igazán szükségünk van, és ezt kizárólag megbízható forrásból tegyük. iOS rendszerű eszközök – például iPadek vagy iPhone-ok – esetén ez a megbízható forrás az Apple App Store. Androidos eszközök esetén megbízható forrás a Google Play Store, Amazon tabletek esetén pedig az Amazon App Store. Ugyan képesek lehetünk más forrásból is programokat telepíteni, azonban ezek a külső források sok esetben nem ellenőrzöttek, és sokkal nagyobb eséllyel tartalmaznak vírusos alkalmazásokat. Az is fontos, hogy mielőtt letöltenénk egy appot, mindig ellenőrizzük, hogy van-e róla elég sok pozitív felhasználói vélemény, valamint, hogy az alkalmazás fejlesztője gyakran frissíti-e a programot. Tartózkodjunk a teljesen új vagy kevés értékeléssel rendelkező vagy ritkán frissített alkalmazások használatától.

4. **Adatvédelmi funkciók**: Mobileszközeink folyamatosan rengeteg információt gyűjtenek rólunk, mivel szinte mindig velünk vannak. Alaposan nézzük át eszközeink adatvédelmi beállításait – mint például a tartózkodási helyzetünk nyomon követése – és bizonyosodjunk meg arról, hogy a szenzitív információkat tartalmazó értesítések – például a biztonsági kódok – nem jelennek meg a zárolt képernyőn.
5. **Munkahelyi használat**: Bizonyosodjunk meg arról, hogy csak olyan mobileszközökett használunk munkavégzés céljából, amelyek erre külön engedélyt kaptak. Munkahelyünkön legyünk óvatosak, hogy még véletlenül se készítsünk olyan fotót vagy videófelvételt, ami érzékeny információkat tartalmazhat, például egy fehértábláról vagy a számítógépek képernyőjéről.

Mobileszközeink sokoldalúak, szórakoztatóak és hasznosak. A fenti néhány egyszerű lépés betartásával hosszútávon biztonságban tudhatjuk őket, és ezáltal saját magunkat is.

A szerzőről

Jeroen Beckers mobilbiztonsági szakértő az NVISO-nál, az OWASP MASVS és MSTG biztonsági útmutatók társszerzője, a SANS Intézet oktatója, valamint ő alkotta a SEC575: „Mobileszköz-biztonság és etikus hackelés” című kurzust. Jeroen elérhető a LinkedIn-en https://www.linkedin.com/in/beckersjeroen/.

Források

A frissítés ereje: https://www.sans.org/security-awareness-training/resources/power-updating
Mobilalkalmazások biztonságos használata: https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/
Üzenetküldéses/SMS csalások: https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks
Egyszerű jelszókezelés: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Vishing - Telefonos csaló hívások: https://www.sans.org/newsletters/ouch/vishing

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