

OUCH!

Az Ön havi biztonságtudatossági hírlevele

Mobil készülékek leselejtezése

Áttekintés

A mobil készülékek, mint az okostelefonok, okosórák és tabletek megdöbbentő tempóban fejlődnek tovább, melynek következményeként néhányan szinte évente lecserélik mobil eszközeiket. Sajnos gyakran nem is tudatosul bennünk, milyen sok személyes információ is található ezeken az eszközökön. Az alábbiakban átvesszük, mi minden található a mobil készülékeinken, és hogy miként kellene azt biztonságosan törölni, mielőtt leselejtezzük. Ha a mobil készülékünket a munkaadónk biztosította, vagy bármilyen munkával kapcsolatos adatot tárolunk rajta, mindenképpen egyeztessünk a vezetőnkkel a megfelelő mentéssel és leselejtezéssel kapcsolatos eljárásokról.

Az adataink

A mobil készülékek több érzékeny adatot tartalmaznak, mint a legtöbb ember gondolná: sok esetben jóval többet, mint a számítógépünk:



- Hol élünk, dolgozunk, és milyen helyeket látogattunk meg
- Minden, a telefonkönyvünkben lévő személy elérhetősége, beleértve a családunkét, barátainkét és munkatársainkét
- A hívásnaplónk, ideértve a bejövő és kimenő hívásaink, hangüzeneteink és a nem fogadott hívásaink
- SMS-einket és az alkalmazásokon belüli üzenetváltásainkat, mint például a biztonságos chat alkalmazás, játékok vagy közösségi média
- Böngészési előzményeink, keresési előzményeink, sütik és a lementett weboldalak
- Személyes fényképeink, videóink és hangfelvételeink
- Eltárolt jelszavaink és hozzáféréseink a különböző fiókjainkhoz, mint például a bank, közösségi média vagy email fiókokhoz
- Egészségügyi információink, beleértve a korunkat, szívritmusunkat, fizikai aktivitásunkat vagy a vérnyomásunkat

Töröljük le a készüléket

Függetlenül attól, miként szabadulunk meg a mobil készülékünktől □ elajándékozunk, elcseréjük egy újabbra, átadjuk egy családtagunknak, tovább értékesítjük, vagy csak eldobjuk □ mindenképp előtte meg kell bizonyosodnunk arról, hogy minden adatunkat biztonságosan letöröltük a készülékről. Az egyszerű törlés nem elégséges, biztonságosan el kell távolítanunk minden adatot a készülékről. Ennek a legkönnyebb módja a készülék gyári beállításokra történő visszaállítás (ún. reset funkció). A reset funkció a készüléktől függetlenül különböző helyen lehet elérhető, alább megtaláljuk két leggyakoribb operációs rendszerrel használatos lépéseket. Még biztonságosabb, ha engedélyezzük a készüléktitkosítást, mielőtt reseteljük azt. A legtöbb új készülék

esetében a legkönnyebben úgy tudjuk ezt végrehajtani, ha engedélyezzük a képernyőzárat (amit remélhetőleg már régen meg is tettünk). Végezetül erősen javasolt a készülék lementése a resetelést megelőzően.

- Apple iOS eszközök: Beállítások | Általános | Visszaállítás | Összes tartalom, beállítás törlése
- Android eszközök: Beállítások | Adatvédelem | Gyári adatok visszaállítása

SIM és külső kártyák

A készüléken túlmenően azt is fontolóra kell vennünk, hogy mit teszünk a SIM (Subscriber Identity Module) kártyánkkal. A készülékek a SIM kártyát használják arra, hogy felépítsék a mobil- vagy adatkapcsolatot. Amikor reseteljük a készülékünket, a SIM kártya továbbra is őriz információkat az előfizetésünkről, ami hozzánk kötődik. Ha megtartjuk a hívószámunkat, és csak egy új készülékre váltunk, akkor egyeztessünk a szolgáltatónkkal a kártya átvitelével kapcsolatban. Amennyiben ez nem lehetséges, tartsuk meg a SIM kártyánkat, és fizikailag semmisítsük meg annak érdekében, hogy megelőzzük, hogy valaki más megszemélyesítsen minket a segítségével, és hozzáférést nyerjen a számlánkhöz vagy előfizetésünkhöz. Végezetül fontos kiemelni, hogy néhány Android eszköz a kivehető SD (Secure Digital) kártyát is felhasználja a tárhely kiterjesztéséhez. Az ilyen külső, eltávolítható kártyákat vegyük ki, mielőtt megválnánk a készüléktől, ezek ugyanis gyakran újra felhasználhatóak az új készülékben, vagy általános adattárolásra is alkalmazhatóak a számítógépén egy USB adapter segítségével. Ha az SD kártya újrafelhasználása nem lehetséges, akkor a régi SIM kártyához hasonló módszerrel, fizikailag semmisítsük meg.

Amennyiben bizonytalanok vagyunk a fenti lépések valamelyikében, vagy a készülékünk reset funkciója máshol érhető el, vigyük el a készüléket az üzletbe, ahol vásároltuk, és kérjük egy képzett technikus segítségét. Végezetül, amennyiben mindössze el akarjuk dobni a telefonunkat, inkább fontoljuk meg az elajándékozását. Sok kiváló jótékonyági szervezet fogad el használt mobil készülékeket, és sok szolgáltatónak van erre a célra kialakított adománygyűjtő ládája is a boltjaikban.

Magyar Kiadás

A Nemzeti Kibervédelmi Intézet (NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. A Nemzeti Kibervédelmi Intézet rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a <http://www.govcert.hu/> és a <http://neih.gov.hu> oldalon olvasható.

A szerzőről

Christopher Crowley (@CcrowMontabce) egy független konzultáns Washington DC-ből, szakterülete a biztonságos üzemeltetés. Esetenként tweetel és blogol is. Figyelemmel követhetjük a kiberbiztonsági műveleti központokról (Security Operations Center – SOC) szóló, nemsokára megjelenő könyvét is. Christopher vezető tanár a SANS intézetben.



Hivatkozások

- SANS tanfolyam: Pen Testing Mobile Devices: <https://sans.org/sec575>
- SANS tanfolyam: Advanced Smartphone Forensics Course: <https://sans.org/for585>
- FTC tanácsok a mobil készülékek leselejtezéséről: <https://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device>

Az OUCH! a Sans Security Awareness részleg által közzétett és a [Creative Commons BY-NC-ND 4.0 licenz](https://creativecommons.org/licenses/by-nc-nd/4.0/) alapján terjesztett hírlevél. A hírlevél szabadon terjeszthető vagy tudatosító programokban felhasználható mindaddig, amíg az nem kerül módosításra. A Fordításért vagy további információért lépjen kapcsolatba velünk a www.sans.org/security-awareness/ouch-newsletter címen. Szerkesztette: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Fordította: Tikos Anita