

OUCH!

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Így szabaduljunk meg a mobilkészülékeinktől

Áttekintés

A mobilkészülékek, mint például az okostelefonok, az okosórák és a táblagépek elképesztő ütemben fejlődnek és újulnak meg folyamatosan. Ennek eredményeképpen akár évente is lecserélhetjük készülékeinket. Sajnos nem is vagyunk tudatában annak, hogy milyen sok személyes adatot tárolunk mobilkészülékeinken — sokkal többet, mint a számítógépünkön. Az alábbiakban bemutatjuk a mobilkészülékeinken található különböző adattípusokat, illetve azt, hogy hogyan törölhetjük biztonságosan készülékeinket, mielőtt azokat kidobnánk vagy lecserélnénk. Ha munkahelyüinktől kaptuk a mobilt, először mindenképpen egyeztessünk felettesünkkel a készülék leadásának eljárásáról!

A készülékeken tárolt adataink

Mobilkészülékeink több érzékeny adatot tárolnak, mint gondolnánk, többek között...

Azt, hogy hol élünk és dolgozunk, valamint a napi utazási szokásainkat.

A címjegyzékünkben szereplő személyek elérhetőségeit, beleértve családtagjainkat, barátainkat és kollégáinkat.

Telefonhívásaink előzményeit, a hangpostán hagyott üzeneteket, a bejövő, kimenő és nem fogadott hívásokat.

Csevegéseinket a chat applikációkból, játékokból és a közösségi média appokból.

Személyes fotókat, videókat és hangfelvételeket.

Tárolt jelszavainkat és hozzáféréseket a különböző fiókjainkhoz (banki, közösségi média, e-mail) való hozzáférést.

Egészséggel kapcsolatos információkat, beleértve életkorunkat, pulzusunkat vagy az edzési előzményeinket.

Pénzügyi információkat, például hitelkártyák, fizetési módok vagy tranzakciók adatait.

Az adatok törlése

Függetlenül attól, hogy hogyan tervezünk megszabadulni az eszközünktől – elajándékoznánk, lecserélnénk, eladnánk vagy akár újrahasznosítanánk –, először töröljük le róla az érzékeny adatokat! Ne feltételezzük, hogy a következő tulajdonos majd „helyesen fog cselekedni”. Első lépésként készítsünk biztonsági mentést a készülékről, hogy vissza tudjuk állítani, illetve át tudjuk vinni az összes adatot és beállítást az új eszközünkre. Ha megvan a biztonsági mentésünk, állítsuk alaphelyzetbe a készüléket, ezzel letöröljük róla az összes adatot, és visszaállítjuk a gyári alapbeállításokat. Az alaphelyzetbe állítási folyamat során előfordulhat, hogy az eszköz, felhőszolgáltatásunk jelszavának megadására kér minket annak érdekében, hogy megszakítsa az eszköz és a felhő közötti kapcsolatokat; ezt mindenképpen tegyük meg! Az alábbi visszaállítási lépések a két leggyakoribb eszközre – Apple és Android – telefonokra vonatkoznak.

Apple iOS eszközök: Beállítások | Általános | Átvitel vagy visszaállítás | Minden tartalom és beállítás törlése.

Android készülékek: Beállítások | Rendszer | Beállítások visszaállítása | Minden adat törlése (ezek az opciók a készülék gyártójától függően változhatnak).

SIM és külső kártyák

A készülék visszaállítása mellett fontoljuk meg azt is, hogy mi legyen a SIM -kártyánkkal. Ez az a kis kártya a telefonunkban, amit a telefonszolgáltatótól kapunk, azonosítja a készülékünket és lehetővé teszi, hogy mobil- vagy adatkapcsolatot létesítsünk. Amikor letöröljük készülékünket, a SIM-kártya továbbra is megőrzi a fiókunkra vonatkozó információkat, mivel ez hozzánk van kötve. Ha megtartjuk a telefonszámunkat és új készülékbe költözünk, egyeztessünk telefonszolgáltatónkkal a SIM-kártya átviteléről! Ha ez nem lehetséges, tartsuk meg a régi SIM-kártyát, és fizikailag semmisítsük meg! Sok mai modern okostelefon rendelkezik úgynevezett eSIM-mel, ami egy virtuális SIM-kártya, szemben a fizikai SIM-kártyával. A visszaállítás során az eSIM is törlődik.

Végezetül, néhány Android mobilkészülék cserélhető SD (Secure Digital) kártyát használ a plusz tárhely biztosításához. Távolítsuk el ezeket a külső tárolókártyákat az eszközről, mielőtt végleg eldobjuk a készüléket! Ezek a kártyák általában újrafelhasználhatóak új mobilkészülöknél, vagy egy USB-adapterrel általános tárolóként is használhatók számítógépünkön. Ha az SD-kártya újrafelhasználása nem lehetséges, akkor a régi SIM-kártyához hasonlóan javasoljuk a kártya fizikai megsemmisítését.

Ha nem vagyunk biztosak a fent említett lépések valamelyikében vagy ha ezektől eltérő visszaállítási opciókkal rendelkezünk, vigyünk vissza a mobilkészüléket abba az üzletbe, ahol vásároltuk, és kérjünk ott segítséget! Végül, ha a készülék kidobása mellett döntünk, előtte fontoljuk meg az eladományozás lehetőségét is! Számos jótékonyági szervezet fogadja szívesen a használt mobilkészülékeket, és sok mobilszolgáltatónak van az üzleteiben erre kijelölt leadási pontja.

A szerzőről

Heather Mahalik (@HeatherMahalik) is the Sr. A Cellebrite digitális intelligenciáért felelős igazgatója és a SANS DFIR tanterv vezetője [FOR585](#) szerző és társoktató a SANS-nál. Heather karrierje nyomelemzői kutatásokon és 20 évnyi esetmunkán alapszik. Blogja itt érhető el: www.smarterforensics.com/blog.



Források

Mobilalkalmazások biztonságos használata: <https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/>

Mobilkészülékek biztonságos használata: <https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/>

Mobilkészülék eladományozása: <https://www.makeuseof.com/best-places-to-donate-your-old-phone/>

Fejlett okostelefon forensics SANS kurzus: <https://sans.org/for585>

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

OUCH! A Sans Security Awareness részleg által közzétett és a [Creative Commons BY-NC-ND 4.0](#) licenz, alapján terjesztett hírlevél. A hírlevél szabadon terjeszthető vagy tudatosító programokban felhasználható mindaddig, amíg az nem kerül módosításra. Szerkesztette: Walter Scrivens, Phil Hoffman, Alan Wagoner, Les Ridout, Princess Young.