

MEGKÉRDEZTÜK

Hogy lehet **BIZTONSÁGOS** a használt telefon **ELADÁSA**

Tegyük meg a szükséges óvintézkedéseket, nehogy illetéktelen kezekbe kerüljenek az adataink!

A gyári visszaállítás nem elég

A szakember tapasztalatai szerint, a telefon esetében sajnos sokan a legalapvetőbb lépéseket sem teszik meg, ha eladják a készüléküket, ilyen például a fiókokból való kijelentkezés, a gyári alaphelyzetbe való visszaállítás.

„A gyári visszaállítás egyszerűen elvégezhető mind az iPhone, mind az Androidot futtató telefon esetében, a konkrét típusra rákeresve kapunk is erre találatokat a netes keresőkben – magyarázza Csizmazia-Darab István az ESET/Sicontact IT biztonsági szakértője. – Ha mégsem boldogulnánk, mind a két rendszer esetén kérhetünk szakszerű segítséget a mobilszolgáltatóunktól. Ám fontos tudni, hogy ez a visszaállítás nem fizikai, megsemmisítő törlés, hanem csak logikai törlés, emiatt – ha nem történik újabb telepítés – a megfelelő segédprogramok segítségével a látszólag elveszett fájlok jelentős része visszaállítható. Vagyis, az új készüléktulajdonos is próbálkozhat hasonló módszerekkel a mi eladott, továbbadott vagy kidobott mobilunk, USB kulcsunk, tabletünk, laptopunk, merevlemezünk esetében. Ezért, ha extra óvatosság akarunk lenni, érdemes lehet először a telefon titkosítása menüpontot kiválasztani, majd ennek végrehajtása után elvégezni a gyári visszaállítást. Ez egy ideig eltart, viszont cserébe az adatok törlése után már csak titkosított adattöredékek maradnak, amikből nem lehet helyreállítani kulcsokat, jelszavakat, érzékeny adatokat.”

Számítógép, laptop esetében a legbiztosabb, ha kizsereljük és megtartjuk a merevlemez, ez jó szolgálatot tehet külső mentésekhez. Ha mégis továbbadjuk, akkor pedig professzionális adattörlő programmal érdemes (KillDisk, Eraser, Secure Eraser stb.) ezt elvégezni.

FELHŐ ÉS KÖZÖSSÉGI OLDAL

Érdemes lehet jelszavaink biztonságát is áttekinteni.

„Mindenhol legyen egyedi, erős, azaz betűket, számokat és szimbólum karaktereket egyaránt tartalmazó hosszú jelszavunk. Minden helyen, ahol csak lehetőség van rá, alkalmazzunk többlépcsős hitelesítést: biometrikus (pl. arc, ujjlenyomat) azonosítást, egyedi SMS küldést vagy egyéb hitelesítő alkalmazást. Rendszeres időközönként – akár tapasztaltunk gyanús dolgokat, adatszivárgást, akár nem – cseréljük a legfontosabb fiókjaink jelszavait, eladáskor pedig ezt mindenképpen tegyük meg!

A felhős tárhelyekre is érdemes alkalmazni a fentieket, vagyis erős jelszót választani, kétféle hitelesítést alkalmazni mindenhol, ahol ez csak lehetséges, illetve a jelszó cseréje is jó ötlet.

„A jelszó érték, bizalmas adatainkat, belépési hitelesítéseinket, személyes fájljainkat védelmezi. Sok szolgáltatásnál – például Gmail, Facebook, LinkedIn – kérhetünk értesítést, ha valaki a nevünkben megpróbál a fiókunkba bejelentkezni.

Érdemes ezekre nagyon odafigyelni, és azonnali jelszócserével, többtényezős hitelesítés bekapcsolásával reagálni.”

Pénzünk bánhatja

A banki ügyeket ma már sokan mobilkészülökről intézik. Amellett, hogy eladáskor titkosítással és a gyári alaphelyzetbe állítással a banki adatainkat is védhetjük, fontos amúgy is betartanunk néhány biztonsági szabályt.

- **Mindig saját, megbízható eszközünkről lépünk be, emellett csak biztonságos internetkapcsolattal tegyük ezt!**
- **Minden készüléken fusson naprakész vírusvédelmi program!**
- **Legyünk tudatosak, ne dőljünk be az adathalász és egyéb csalásoknak, használat után mindig jelentkezzünk ki a banki szolgáltatásokból!**
- **Hasznos, ha aktiváltatjuk bankunknál az SMS vagy push üzenet alapú azonnali egyenlegértesítést, mert így értesülünk a számlánkon zajló összes pénzmozgásról, és sokkal könnyebben felfigyelhetünk az esetleges gyanús tevékenységekre.**
- **Ugyancsak hasznos biztonsági lépés, ha az internetes vásárlásokhoz virtuális kártyát igényelünk.**