13. Egy vállalkozás okostelefonokkal szerelné fel a dolgozóit. Szeretnék azonban mind a készülékeket, mind pedig a rajtuk lévő bizalmas adatokat a lehető legnagyobb biztonságban tudni. Milyen hardveres és szoftveres megoldásokat, karbantartási tevékenységeket javasolna a készülékek és az adatok megvédésére akár meghibásodás, akár pedig a készülék elvesztése vagy ellopása esetére?

Kulcsszavak, fogalmak:

– jelszózárak, blokkolás jelszó próbálkozás esetén

– biometrikus azonosítás

– adatok biztonsági mentése felhő tárhelyre

– helymeghatározó alkalmazás

– távoli blokkolás és távoli törlés

– vírusvédelem

– operációs rendszer és alkalmazás frissítés

MOBILTELEFON VÉDELEM ÉS BIZTONSÁG

Mivel a telefonunkat egyre több dologra használjuk, egyre több fontos és személyes adatot kezelünk a készülékünkön. Az adataink védelme, azaz a biztonságos használat nem nyilvánvaló dolog sokak számára ezért összeszedtünk néhány jó tanácsot ebben a témában.

Jelszó

Ha jelszót használunk a belépéshez, akkor erős jelszó legyen, azaz legyen benne kis- és nagybetű, szám, különleges karakterek, minimum 8 hosszú és ne legyen igazi szavak kombinációja vagy származéka. Az a legjobb ha rendszeresen változtatjuk a jelszavainkat.

Képernyő zárolás/feloldás

Ha a kijelzőre rajzolást választjuk a belépéshez, akkor a kijelzőt rendszeresen tisztítsuk, mert különben a sok használattól a kijelzőn a titkos jelünk látszódni fog.

Arcfelismerés

Alapból figyelni kell arra, hogy a referencia kép jó megvilágításban készüljön, különben hasonló arcokra is kinyitja az eszközünket a rendszer. A felismerés egyelőre nem megbízható, de alap védelemnek el megy.

Ujjlenyomat

Több mintát adjunk le, ne elégedjünk meg az 1-2 mintával, mert lehet, hogy csak töredékét mentette el az ujjlenyomatunknak, ami miatt akár idegenek is fel tudják oldani ezt a zárat!

Kijelzőzár

Állítsuk be, hogy kapcsolódjon be a kijelzőzár, amikor nem használjuk a telefont. Egyes banki alkalmazások addig nem is működnek, ameddig ez nincs bekapcsolva.

Ellenőrzött alkalmazások

Csak hivatalos helyekről (Google Play, App Store, Galaxy Store, etc.) töltsünk le alkalmazásokat, mert azok megbízhatóbbak. Ha csak úgy letöltünk az internetről, akkor nagy a kockázata, h fertőző, kárt okozó vagy adatot lopó alkalmazást rakunk fel a telefonunkra.

Frissítések

Rendszeresen (alapból automatikusan) frissítsük az operációs rendszert, valamint az alkalmazásokat is. Abban az esetben, ha a frissítés oldalra lépve találunk még nem frissített alkalmazást és éppen ráérünk, akkor érdemes kézzel elindítani a frissítést. Persze csak akkor ha Wi-Fi-n vagyunk, vagy olyan a mobil-NET elérésünk, hogy akár egy nagyobb letöltés is belefér.

Nem használt alkalmazások törlése

Minél kevesebb alkalmazás van a telefonunkon, annál kisebb a kockázata, hogy egy alkalmazás jó vagy rossz hiszeműen biztonsági rést képez számunkra.

Biztonsági másolat

Bár egyesek szerint megvéd, de aktív/automatikus frissítés esetén sajnos az új hibák (például zsaroló titkosítás) is átkerülhet a másolatba. Innentől a védelem nem ér semmit sem! Ennek ellenére, bár tökéletes védelem soha sincs, a rendszeren mentés jó ötlet.

Állitsuk le a GPS-t, Wifi-t és a Bluetooth-ot!

Ezeket csak akkor kapcsoljuk be, amikor szükségünk van rájuk es használat után kapcsoljuk is ki őket.

Készülék követése

Például Samsung telefonokon megtalálható a Find My Mobile funkció, aminek a segítségével a https://findmymobile.samsung.com oldalon lehet követni a telefont. Ezzel távolról lehet a készüléket feloldani és követni a helyét meg akkor is ha a készüléknek nincs internet kapcsolata.

Adatok titkosítása

Android rendszerrel futó készülékeken van lehetőség az adatok titkosítására. A használata picit lassítja a készüléket, szóval csak nagyobb kapacitású telefonoknál érdemes ezt bekapcsolni. A használata PIN kódot igényel és PIN nélkül nem lehet az adatokhoz hozzáférni, ilyenkor legrosszabb esetben csak a gyári beállítások visszaállításával lehet újra használatba venni a készüléket.

Alkalmazások jogosultságai

Ellenőrizzük, hogy a különböző alkalmazások mihez férnek hozzá (kamera, lokáció, tárhely, stb.) és minden hozzáférést töröljünk, amire csak nincs szükség.

Google személyre szabott reklám szolgáltatásai

Ezek a szolgáltatások plusz funkciót jelentenek, de több adatot is gyűjtenek rólunk. Érdemes alaposan elgondolkodni, hogy mire van szükségünk és ennél többet nem engedélyezni.

Fájlok és könyvtárak titkosítása

Ha az operációs rendszerünk nem kínálja ezt alap funkcióként, sokszor a gyártó ad hozzá ilyen funkciót (pl. Samsung Secure Folder), illetve vásárolhatok erre a célra készült alkalmazásokat.

Helyelőzmények kezelése

A Google-fiókban kikapcsolható és akkor a Google nem jegyzi meg, hogy mikor merre jártunk.

Víruskereső programok

Sok alkalmazás közül választhatunk, a nagy nevek (Avast, AVG, Kaspersky, ESET, stb.) nagyon jó és többnyire ingyenes lehetőségeket kínálnak. A legfontosabb, hogy állítsuk be, hogy a fenyegetések adatbázisa automatikusan frissüljön.

Vigyázzunk a telefonunkra

Utolso pontként megemlítenénk a legalapvetőbb, de mégis legfontosabb tanácsot, mégpedig azt, hogy ne hagyjuk őrizetlenül a telefonunkat és ne rakjuk olyan zsebbe, ahonnan egy zsebtolvaj könnyen kilophatja.