



ELBIR

Elektronikus Lakossági Bűnmegelőzési Információs Rendszer

2018. február



„Egy hónap - egy téma a biztonságos internethasználatért”, az Országos Rendőr-főkapitányság bűnmegelőzési felhívása

A mobil eszközök biztonsága

A mobil eszközök (okostelefonok, tabletek) jelentősen megkönnyítik mindennapjainkat. Mivel nem csak otthon vagy a munkahelyünkön használjuk, ezért nagyobb a kockázata, hogy illetéktelen kezekbe kerülnek. Bizalmas és személyes adatokat tárolunk rajtuk, így elvesztésük vagy ellopásuk esetén az illetéktelen személyek hozzáférhetnek az eszközön tárolt e-mailekhez, üzenetekhez, fényképekhez, videókhoz, személyes és bankkártya adatokhoz, valamint banki és közösségi oldalak bejelentkezési adataihoz. A jogosulatlan hozzáféréstől adódó kockázatok elkerülése érdekében gondoskodjunk mobil eszközeink megfelelő védelméről!

KÉPERNYŐZÁR

Ha az eszközünk illetéktelen személy kezébe kerül, megfelelő védelem hiányában nagyon könnyen hozzáférhet adatainkhoz. Ennek megelőzésére a legegyszerűbb, ha bekacsoljuk az automatikus képernyőzárát, így ha nem használjuk az eszközt, az előre beállított idő után a képernyőzár automatikusan bekapcsol. A feloldása történhet jelszó beírásával, pontokat összekötő minta lerajzolásával, vagy ujjlenyomattal. Amennyiben az eszközben van SIM kártya, ahhoz is kapcsoljuk be a PIN kódot!

TÁVOLI FELÜGYELET BEÁLLÍTÁSA

A távoli felügyelet használata esetén – amennyiben az eszköz be van kapcsolva és csatlakozik az internethez – lehetőség van az eszköz helyének térképen történő megjelenítésére, illetve szükség esetén az eszközön tárolt felhasználói adatok és beállítások törlésére. Az ehhez szükséges alkalmazás az alkalmazásboltból letölthető.

FRISSÍTÉSEK ÉS BIZTONSÁGI BEÁLLÍTÁSOK

Frissítse mobil eszközei operációs rendszerét, az erre vonatkozó figyelmeztetést követően minél hamarabb! Az alkalmazások esetében engedélyezze, hogy automatikusan frissítsék magukat! A frissítések kritikus biztonsági réseket javíthatnak. A ki nem javított hibákat a hackerek kihasználhatják rosszindulatú programok telepítésére, bizalmas adatok megszerzésére. Ha nem használja a wifit vagy a Bluetooth-t, kapcsolja ki ezeket, így is korlátozhatja az eszköz illetéktelen elérését!

ADATOK BIZTONSÁGA

A mobil eszközön tárolt adatokhoz nem csak az eszköz megszerzésén keresztül lehet hozzájutni. Sok alkalmazás menti és szinkronizálja az adatokat (fájlokat, beállításokat, jelszavakat) valamilyen online tárhelyre (másképpen felhőbe).

Ez akár hasznos is lehet, hiszen az eszköz elvesztése vagy ellopása esetén az adatok nem vesznek el, azok a felhőből elérhetőek. Fontos azonban, hogy a szinkronizáció csak a tudtunkkal és beleegyezésünkkel történjen. Ha nem tartjuk szükségesnek az adott alkalmazásban az adatok szinkronizálását, akkor azt tiltsuk le!

BIZTONSÁGOS ALKALMAZÁSOK

A mobil eszközön futó alkalmazások – a részükre biztosított engedélyektől függően – hozzáférhetnek a személyes adatokhoz, fájlokhoz, fényképekhez, videókat, hangfelvételt készíthetnek, ezeket továbbíthatják az alkalmazás készítőinek. Az alkalmazások biztonságos használata érdekében célszerű az alábbi ajánlások betartása.

- Mobilalkalmazásokat mindig a hivatalos alkalmazás-áruházból töltsünk le! Ellenőrizzük, hogy az eredeti alkalmazásról van-e szó! A bűnözők hasonló neveket használnak, hogy megtévesszék a felhasználókat.
- E-mailben, üzenetben kapott linkről ne töltsünk le alkalmazásokat!
- Letöltés előtt ellenőrizzük az alkalmazás és a gyártó értékelését is! Szánjunk rá időt és olvassuk el a felhasználók véleményét! Ha rossz értékelést kapott az alkalmazás, ne töltsük le! Válasszunk olyan alkalmazást, amit sokan töltöttek le és pozitív értékeléssel bírnak!
- Ellenőrizzük, hogy milyen engedélyeket kér az alkalmazás! Ha nem tartjuk szükségesnek, akkor ne töltsük le (pl. navigációs és térkép programoknak szükségük lehet hozzáférni a telefon helyzetéhez, de zenelejátszóknak már nem)!

BIZTONSÁGOS HASZNÁLAT

- A böngészőbe ne mentse el a felhasználói nevét, jelszavát! Használjon jelszókezelő alkalmazást!
- A böngészőben megjelenő figyelemfelhívások (az eszköz fertőzött, töltsön le vírusirtót, az eszköz elavult, frissítse) célja, hogy valamilyen kártékony programot telepítsen az eszközre. Ilyen esetben ne töltsön le semmit, és zárja be a böngészőt!

VAS MEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNÜGYI IGAZGATÓSÁG
BŰNÜGYI OSZTÁLY
Bűnmegelőzési Alosztály

9700 Szombathely, Petőfi S. u. 1/C.
Telefon: 06/94/521-065 Fax: 06/94/521-160
E-mail: bunmeg.vasmrk@vas.police.hu