



ELBIR
Elektronikus Lakossági Bűnmegelőzési Információs Rendszer



Biztonsági tanácsok mobilkészülékekhez

Legyen szó laptopról vagy okostelefonról, a bűnözőket mind a készülék, mind pedig a rajtuk található érzékeny adatok érdeklik. A védelem első pontja a fizikai hozzáférés: munkahelyen, tárgyaláson, étteremben, reptéren, szállodában, **készülékünket mindig tartsuk látótávolságban, kartávolságunkban.**



Használjanak jelszavas vagy PIN zárolás feloldást, mely hozzáférés védelmet biztosít, ha idegen kézbe kerülne a készülék.



Az időzár, képernyő időkorlát opciót kapcsolják be, így illetéktelenek nem tudják megtekinteni címjegyzéküket illetve egyéb személyes adataikat, hívást indítani vagy alkalmazásokat telepíteni. *(vicces kedvű kollégák sem tudják telefonunk nyelvét kínaira változtatni)*



Kapcsolják be az **adatok törlése opciót** bizonyos számú (pl. 5) **sikertelen feloldási próbálkozást követően**. Így ha el is tulajdonítják a készüléket, legalább személyes illetve céges adataikat biztonságban tudhatják.



Ha befejezték használatát, **kapcsolják ki a Bluetooth, Wi-Fi kommunikációt**. Ezzel az akkumulátor készenléti idejét növelhetik, valamint elkerülhetik a csaló hotspot-okra való csatlakozást illetve kényszerítő Bluetooth üzenetek fogadását. Wi-Fi esetében ajánlott továbbá az **„Automatikus csatlakozás”/ „Hálózati értesítés” kikapcsolása**.



Alkalmazások telepítését csak a hivatalos áruházakból (Google Play, Apple Store) végezzék. Ezek sem tökéletesek, de biztonságosabbak, mint a kontroll nélküli forrásból származók.



BÁCS-KISKUN MEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNMEGELŐZÉSI OSZTÁLY
KECSKEMÉT

6000 Kecskemét, Batthyány u. 14., Postacím: 6001 Kecskemét, Pf.:302 Tel:76/513-300/30-27, BM: 33/30-27, Fax: 76/513-300/30-98 BM 33/30-98, Mobil: +3620/560-5146
e-mail: elbir@bacs.police.hu web: <http://www.police.hu/hirek-es-informaciok/bunmegelozes>

 **Alkalmazások engedély** kéréseit mindig olvassák el. Ha pl. egy játék túl kíváncsi, és a működéséhez józanésszel végiggondolva egyáltalán nem szükséges – pl. SMS küldés, címjegyzékhez hozzáférés -felhatalmazásokat is szeretne, inkább álljanak el a telepítéstől és keressenek alternatívát.

 **Nyilvános Wi-Fi használata során mellőzzék a vásárlást, vagy banki oldalak használatát.** Ilyen hálózati kapcsolat során kerüljék az olyan kommunikációt, mely jelszót, számlaszámot, kártyaszámot érint, hiszen ezeket akár mások is láthatják.

 Legyenek **körültekintőek a QR kódok** (kétdimenziós vonalkód) **feldolgozásával.**



 Telepítsenek és **használjanak** valamilyen **antivírust vagy biztonsági csomagot.** (használjanak pl. avast!, F-Secure, Kaspersky vagy Symantec terméket)

Böngészés során kiemelten figyeljenek (kétszer is ellenőrizzük a címsort) a megnyitott oldalra, hiszen a kis képernyő miatt könnyebben eshetnek adathalászat áldozatává.



 **Alkalmazásaik védelme** fontos. Például az AppLock alkalmazás lehetővé teszi, hogy kiválasztott funkciók csak egy külön jelszó begépelése után legyenek aktíválhatók.

 **Adataik védelme, titkosítása.** Kapcsolják be a készüléken valamint a külső SD kártyán található adatok titkosítását.

Android



IOS (iPhone, iPad)



Windows Phone



Forrás: https://www.mkb.hu/sw/static/file/item_5137.pdf
Képek: internet