Biztonsági tanácsok mobilkészülékekhez

Legyen szó laptop-ról 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.**

	Jelszavas vagy PIN zárolás feloldást használjunk, mely hozzáférés védelmet biztosít, ha idegen kézbe kerülne a készülék. **Az időzár, képernyő időkorlát opciót kapcsoljuk be**, így illetéktelenek nem tudják megtekinteni címjegyzékünket illetve egyéb személyes adatainkat, hívást indítani vagy alkalmazásokat telepíteni. *(vicces kedvű kollégák sem tudják telefonunk nyelvét kínaira változtatni)*
	Kapcsoljuk be az **adatok törlése opció**t bizonyos számú (pl. 5) **sikertelen feloldási próbálkozást követően**. Így ha el is tulajdonítják a készüléket, legalább személyes illetve céges adatainkat biztonságban tudhatjuk.
	Ha befejeztük használatát, **kapcsoljuk ki a Bluetooth, Wi-Fi** kommunikációt. Ezzel az akkumulátor készenléti idejét növelhetjük, valamint elkerülhetjük a csaló hotspot-okra való csatlakozást illetve kéretlen Bluetooth üzenetek fogadását. Wi-Fi esetében ajánlott továbbá az „**Automatikus csatlakozás**”/ „**Hálózati értesítés**” **kikapcsolása**.
	Alkalmazások telepítését csak a hivatalos áruházakból (Google Play, Apple Store) végezzük. Ezek sem tökéletesek, de biztonságosabbak, mint a kontroll nélküli forrásból származók. **Alkalmazások engedély** kéréseit mindig olvassuk el. Ha pl. egy játék túl kíváncsi, és a működéséhez józanésszel végiggondolva egyáltalán nem szükséges – pl. SMS küldés, címjegyzékhez hozzáférés - felhatalmazásokat is szeretne, inkább álljunk el a telepítéstől és keressünk alternatívát.
	Nyilvános Wi-Fi használata során mellőzzük a vásárlást, vagy banki oldalak használatát. Ilyen hálózati kapcsolat során kerüljük az olyan kommunikációt, mely jelszót, számlaszámot, kártyaszámot érint, hiszen ezeket akár mások is láthatják. Legyünk **körültekintőek a QR kódok** (kétdimenziós vonalkód) **feldolgozásával.** 
	Telepítsünk és **használjunk** valamilyen **antivírust vagy biztonsági csomagot.** *(használjunk pl. avast!, F-Secure, Kaspersky vagy Symantec terméket)* Böngészés során kiemelten figyeljünk (kétszer is ellenőrizzük a címsort) a megnyitott oldalra, hiszen a kis képernyő miatt könnyebben eshetünk adathalászat áldozatául.
	Alkalmazásaink védelme fontos. Például az AppLock alkalmazás lehetővé teszi, hogy kiválasztott funkciók csak egy külön jelszó begépelése után legyenek aktiválhatók.
	Adataink védelme, titkosítása. Kapcsoljuk be a készüléken valamint a külső SD kártyán található adatok titkosítását.

Android **iOS** (iPhone, iPad) **Windows Phone**