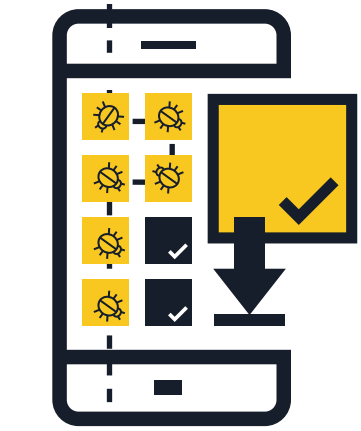
MOBILTELEFONOKON FUTÓ KÁRTEVŐ PROGRAMOK

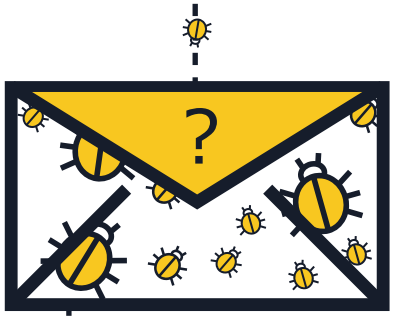
TIPPEK ÉS TANÁCSOK A VÉDEKEZÉSHEZ



1 Csak megbízható forrásokból származó alkalmazásokat telepítsen

- **Megbízható alkalmazásboltban vásároljon** — Az alkalmazás letöltése előtt keressen rá magára az alkalmazásra és annak gyártójára is. Legyen körültekintő az e-mailben vagy szöveges üzenetben érkező, külső fél vagy ismeretlen forrás alkalmazásainak telepítését kérő felhívásokkal.
- **Ha vannak visszajelzések,** érdemes megnézni, hogy a többi felhasználó milyen véleménnyel van az adott alkalmazásról.
- **Olvassa el, hogy milyen engedélyeket kér az alkalmazás** — Nézze meg alaposan, hogy milyen típusú adatokhoz férhet hozzá az alkalmazás, és ellenőrizze azt is, hogy megoszthatja-e azokat külső féllel. Ha a feltételekkel nem ért egyet, vagy gyanúsnak tűnnek, ne töltse le az alkalmazást.

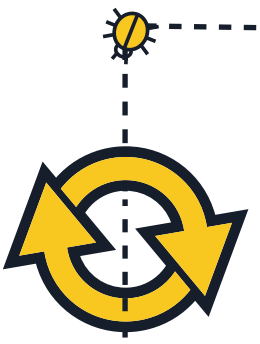
2 Ne kattintson a kéretlen szöveges vagy e-mail üzenetekben lévő hivatkozásokra vagy mellékletekre



- **Ne bízzon a kéretlen e-mailekben vagy szöveges üzenetekben (SMS és MMS) lévő hivatkozásokban** — Megérkezésük után azonnal törölje őket.
- **Nagyon alaposan ellenőrizze a rövidített URL-címeket és a QR-kódokat** — Előfordulhat ugyanis, hogy kártékony weboldalakra vezetnek, vagy közvetlenül kártevő szoftvert töltenek le az eszközre. Mielőtt a hivatkozásra kattintana, az URL-eket szűrő oldalon ellenőrizze, hogy a céloldal valós webhely-e. QR-kód esetén, a QR-kódot olyan olvasóval olvassa be, amely előnézetben megjeleníti a kódba ágyazott webhely címét, és használjon mobilbiztonsági programot, amely figyelmeztet a kockázatos hivatkozásokra.

3 Fizetést követően jelentkezzen ki a weboldalakról

- **A mobilböngészőkben és -alkalmazásokban sehol nem szabad menteni a felhasználónevet és a jelszót** — Ha a telefont elveszti vagy ellopják, bárki be tud lépni a fiókba. Ha a tranzakció befejeződött, a böngészőablak bezárása helyett először jelentkezzen ki az oldalról.
- **Nyilvános Wi-Fi hálózaton keresztül ne lépjen be netbankjába, és ne vásároljon a neten** — Netbankos műveleteket és vásárlásokat csak megbízható hálózaton keresztül hajtson végre.
- **Ellenőrizze alaposan a weboldal URL-címét** — Bejelentkezés és bizalmas adatok megadása előtt ellenőrizze a webhely címének helyességét. A bank hivatalos netbankalkalmazásának letöltésével biztos lehet benne, hogy mindig valóban a bank hivatalos oldalához csatlakozik.



4 Operációs rendszere és alkalmazásai mindig legyenek naprakészek

- **Amint a rendszer kéri, mindig töltse le a mobileszköz operációs rendszerének frissítéseit** — A naprakész állapotú operációs rendszer nemcsak biztonságosabb, hanem jobban is működik.

5 Ha éppen nem használja, kapcsolja ki a Wi-Fi-t, a helymeghatározási szolgáltatást és a Bluetooth funkciót

■ **Ha nem használja, kapcsolja ki a Wi-Fi funkciót** — Ha a kapcsolat nem biztonságos, az internetes bűnözők könnyen hozzáférhetnek az Ön adataihoz. A hotspotok helyett inkább 3G vagy 4G kapcsolatot használjon. Az adatok titkosításának egyik jól bevált módja a virtuális magánhálózat, azaz a VPN-hálózat alkalmazása.

■ **Csak akkor engedje meg, hogy az alkalmazások használják a helymeghatározási adatokat, ha arra valóban szükség van** — Ezeket az adatokat ugyanis könnyű megosztani és kiszivárogtatni, és előfordulhat, hogy a helyadatok alapján különféle hirdetéseket küldenek Önnek.

■ **Csak akkor legyen bekapcsolva a Bluetooth, ha tényleg használja** — Mindig legyen teljesen kikapcsolva, ne csak „láthatatlan” üzemmódba kapcsolja át. Gyakran előfordul, hogy alapértelmezett beállítás szerint mások simán csatlakozhatnak az Ön készülékéhez anélkül, hogy erről Ön bármit is tudna. A rosszindulatú felhasználók például lemásolhatják az Ön fájljait, hozzáférhetnek a csatlakoztatott készülékekhez, súlyosabb esetben távoli eléréssel hozzáférhetnek magához a telefonhoz is, amelyről drága hívásokat kezdeményezhetnek vagy üzeneteket küldhetnek.

6 Ne adja át másnak személyi adatait

■ **Válaszként soha ne adja meg személyi adatait** olyan megkeresésre, amely látszólag bankjától vagy más hivatalos forrásból érkezik. Ha ilyen megkeresést kap, vegye fel a kapcsolatot a kezdeményező személlyel, és ellenőrizze a kérelem eredetének valódiságát.

■ **REllenőrizze rendszeresen mobilszámláját, hogy van-e rajta esetleg gyanús tétel** — Ha talál olyan tételt, amelyet nem Ön kezdeményezett, azonnal forduljon a mobilszolgáltatójához.

7 Ne módosítsa a készülék szoftverét (jailbreak)

■ Az operációs rendszerek gyártói különféle biztonsági korlátozásokat alkalmaznak, amelyeket eltávolítva teljes hozzáférést lehet szerezni az operációs rendszerhez, illetve annak funkcióihoz (jailbreak). **A készülék biztonsági korlátozásainak eltávolítása (jailbreak) jelentős mértékben csökkentheti a rendszer biztonsági szintjét,** mert olyan biztonsági réseket tesz elérhetővé, amelyekről a felhasználó nem is tudhat.

8 Készítsen adatairól biztonsági másolatot

■ **Sok okostelefon és táblagép lehetővé teszi, hogy az adatokról vezeték nélküli kapcsolaton keresztül biztonsági másolatot készítsen** — Tekintse meg a készülék operációs rendszertől függő lehetőségeket. Az okostelefon vagy a táblagép adatairól készített biztonsági másolatnak köszönhetően az adatok könnyen helyreállíthatók még akkor is, ha a készülék elvész, ellopják vagy az adatok megsérülnek.

9 Telepítse mobilbiztonsági alkalmazást

■ A fertőzés kockázata alól egyik operációs rendszer sem jelent kivételt. Amennyiben lehetséges, **érdemes olyan mobilbiztonsági megoldást alkalmazni,** amely észleli a különféle kémprogramokat és rosszindulatú alkalmazásokat és megakadályozza a településüket, valamint több más, kalózkodás-ellenes és lopásgátló funkcióval rendelkezik.

EUROPOL EC3 European Cybercrime Centre

#MobileMalware