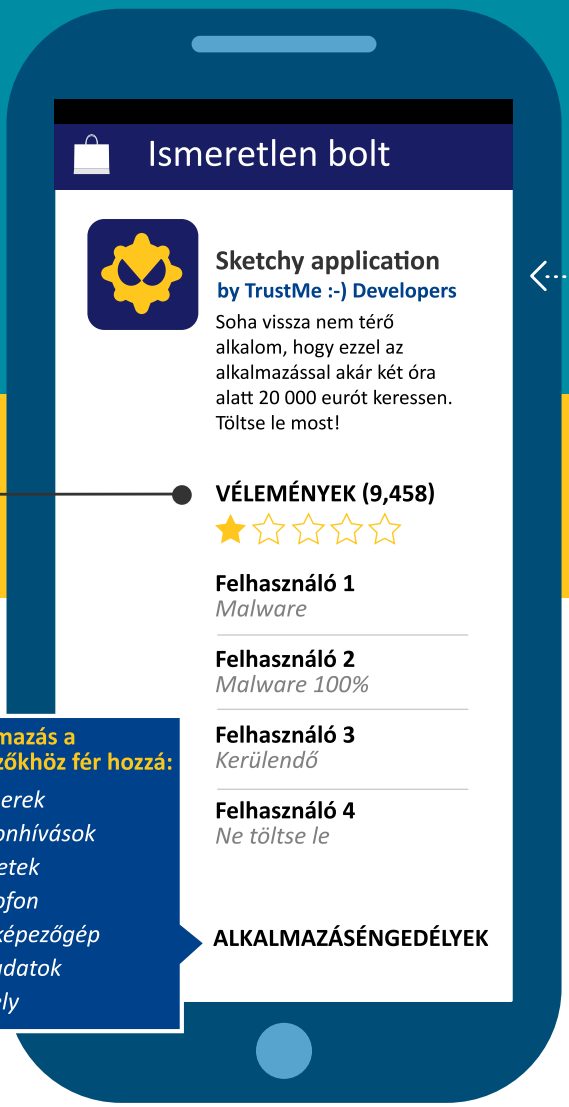
APPS

CSAK EGY JÁTÉKOT?

Csak hivatalos alkalmazásboltból telepítsen alkalmazásokat

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.



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. Az összes engedélyre szüksége van? Ha nem, ne töltse le.

TELEPÍTSEN MOBILBIZTONSÁGI ALKALMAZÁST

Az ilyen programok megvizsgálják az eszközre telepített és a jövőben telepíteni kívánt alkalmazásokat, és értesítenek, ha kártevő szoftvert találnak.

EUROPOL EC3 European Cybercrime Centre | RENDŐRSÉG POLICE | KÉSZENLÉTI RENDŐRSÉG | NEMZETI KIBERVÉDELMI INTÉZET | NMHH Nemzeti Média- és Hírközlési Hatóság | NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

#MobileMalware

MOBILBANKOLÁST ÉRINTŐ KÁRTEVŐ SZOFTVER

A KÁRTEVŐ SZOFTVEREK SOK PÉNZBE KERÜLHETNEK ÖNNEK

A mobilbankolási lehetőségeket kihasználó kártevő szoftverek célja az eszközön tárolt, a pénzforgalommal kapcsolatos adatok megszerzése

HOGYAN TERJED?

- Rosszindulatú oldalak meglátogatása
- Kártevő alkalmazások letöltése
- Adathalászat

MILYEN KOCKÁZATOKKAL KELL SZÁMOLNI?

- Személyi hitelesítő adatok megszerzése
- Jogosulatlan pénzfelvétel

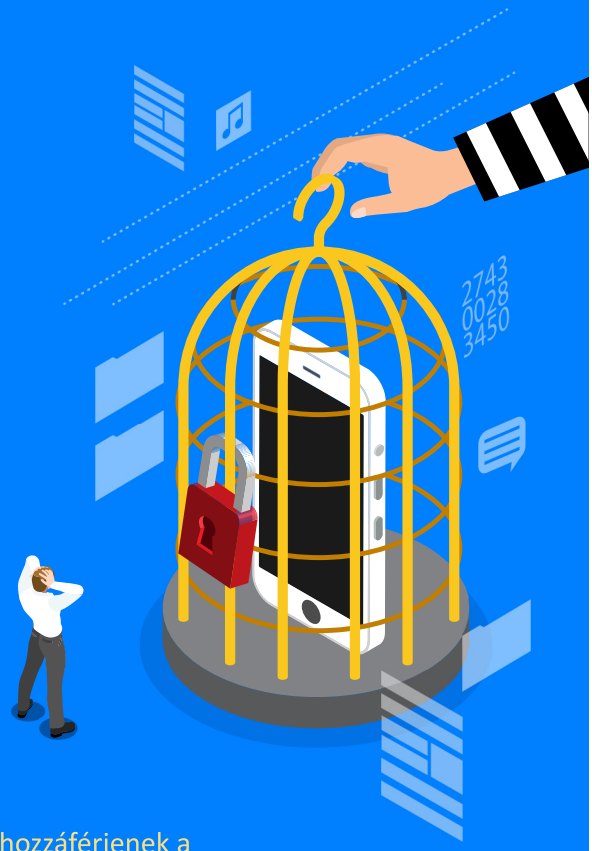
ÖN MIT TEHET?

- Töltse le bankjának hivatalos mobilalkalmazását, és minden alkalommal ellenőrizze, hogy valóban a bank oldalán jár-e. (https://)
- Ne állítsa be úgy a netbankos oldalt vagy az alkalmazást, hogy automatikusan bejelentkezzen.
- Bankkártyájának számát és jelszavát ne adja meg senkinek.
- Ha módja van rá, telepítsen mobileszközére biztonsági programot, amely figyelmezteti a gyanús tevékenységekre.
- Ha elhagyja mobiltelefonját vagy megváltoztatja telefonszámát, értesítse bankját, hogy frissíteni tudják a szükséges adatokat.
- Szöveges üzenetben és e-mailben semmilyen, a számlával kapcsolatos adatot ne osszon meg.
- Bankja netbankos oldalához vagy banki alkalmazásához való csatlakozáshoz mindig biztonságos Wi-Fi hálózatot használjon. Soha ne csatlakozzon nyilvános Wi-Fi hálózaton keresztül!
- Gyakran ellenőrizze bankszámlaegyenlegét.

EUROPOL EC3 European Cybercrime Centre | NEMZETI KIBERVÉDELMI INTÉZET | NMHH | NISZ | #MobileMalware

MOBILESZKÖZÖKÖN
FUTÓ ZSAROLÓVÍRUSOK

ÖSSZES SZEMÉLYES FÁJLJÁNAK BÚCSÚT INTHET



A zsarolóprogramok csak bizonyos összeg megfizetése ellenében teszik ismét elérhetővé a telefonját és a „túszul ejtett” adatokat. Ezek a rosszindulatú programok rendszerint zárolják a készülék kijelzőjét, vagy megakadályozzák, hogy a felhasználók hozzáférjenek a fájlokhoz vagy használhassák a készülék funkcióit.

HOGYAN TERJED?

Fertőzött webhelyek meglátogatásával.

A hivatalos alkalmazások utánzatainak letöltésével.

Adathalász e-mail üzenetekben lévő rosszindulatú hivatkozásra kattintással, vagy ilyen üzenetben érkező melléklet megnyitásával.

MILYEN KOCKÁZATOKKAL KELL SZÁMOLNI?

Előfordulhat, hogy teljesen a gyári alaphelyzetbe kell visszaállítani a készüléket, ami az összes adat elvesztésével is járhat.

A támadó teljes hozzáférést szerezhet a készülékhez, és az azon tárolt adatokat másokkal is megoszthatja.

ÖN MIT TEHET?

Készítsen gyakran biztonsági mentést adatairól, és tartsa alkalmazásait, illetve az operációs rendszert naprakészen.

Lehetőleg ne vásároljon nem megbízható alkalmazásboltokból.

Amennyiben módja van rá, telepítsen a készülékre biztonsági alkalmazást, amely értesíti, ha az eszközt támadás éri.

Legyen óvatos az olyan e-mail üzenetekkel és weboldalakkal, amelyek gyanúsak, vagy túl jól hangzanak ahhoz, hogy igazak legyenek.

Válogassa meg jól, hogy kinek ad az eszközön rendszergazdai jogosultságot.

Ne fizessen váltságdíjat. A kifizetett pénzzel a bűnözőket segíti, és ösztönzést ad nekik, hogy tovább folytassák az illegális tevékenységüket.

EUROPOL EC3 European Cybercrime Centre | RENDŐRSÉG POLICE | NEMZETI KIBERVÉDELMI INTÉZET | NMH Nemzeti Média- és Hírközlési Hatóság | NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

#MobileMalware

WEBALAPÚ FENYEGETÉSEK

JÓL NÉZZE MEG, HOVÁ ÉS MIKOR KATTINT!

Ha a készüléke már nem fog működni, nemcsak személyes adatait veszítheti el, és anyagi veszteségei is lehetnek, hanem a tárolt adatai is elveszhetnek. Ne hagyja, hogy átverjék!

HOGYAN TÖRTÉNHETETT?

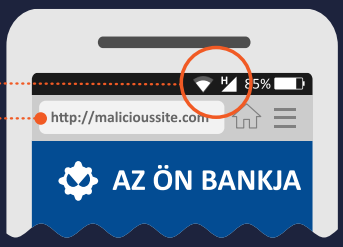
ADATHALÁSZ-TÁMADÁSOK: Az ilyen támadások elkövetői rendszerint magukat megbízható oldalnak vagy cégnek kiadva próbálnak meg személyes adatokat kicsalni a felhasználóktól. A támadások többnyire e-mailben, szöveges üzenetben vagy a közösségi médián keresztül történnek.

INTERNETES BÖNGÉSZÉS: A mobileszköz megfertőződéséhez bőven elég, ha csak egy nem biztonságos oldalt megnyit vele.

FÁJLOK LETÖLTÉSE: Gyakran előfordul, hogy a rosszindulatú hivatkozások és mellékletek e-mail üzenetbe ágyazva jutnak el a felhasználóhoz.

MIÉRT HATÉKONY MÓDSZER EZ?

A mobileszközök FOLYAMATOSAN CSATLAKOZNAK az internethez.



Általános jellegű megszorítást jelent az eszköz kijelzőjének KIS MÉRETE. A mobileszközökön futó böngészőkben az URL-címek csak korlátozott méretben jelennek meg, így sokkal nehezebb ellenőrizni, hogy a cím valódi-e.

A felhasználóknak a mobileszközök SZEMÉLYES BIZTONSÁGÁBA VETETT bizalma.

ÖN MIT TEHET?

Legyen óvatos, ha például egy cég részéről telefonon vagy SMS-ben személyi adatokat kérnek. Ilyenkor érdemes az adott cég hivatalos telefonszámát felhívva ellenőrizni a megkeresés valódiságát.

A mobileszközön való böngészést mindig biztonságos HTTPS-csatlakozáson keresztül végezze. A kapcsolat biztonságos volta az URL-cím első részét megtekintve könnyen megállapítható.

A kéretlen SMS-ben vagy e-mail-üzenetben lévő hivatkozásokra nem szabad rákattintani. Az ilyen üzenetet azonnal törölje.

^Be:%}
W@RY
*)Z#$=

Körültekintően kell akkor is eljárni, ha böngészés közben gyenge nyelvezettel, alacsony felbontással vagy helyesírási hibákkal, elírásokkal sűrűn tarkított oldalra érkezik.

Ha módja van rá, telepítsen mobileszközére biztonsági programot, amely figyelmezteti a gyanús tevékenységekre.

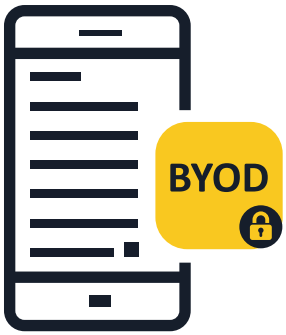
EUROPOL EC3 European Cybercrime Centre | NEMZETI KIBERVÉDELMI INTÉZET | NMHH | NISZ | #MobileMalware

MOBILTELEFONOKON FUTÓ KÁRTEVŐ PROGRAMOK

TIPPEK ÉS TANÁCSOK VÁLLALKOZÁSOKNAK

1 Tájékoztassa a munkatársakat a mobileszközök használatával járó kockázatokról

- A mobileszközöknek köszönhetően mára már igen gyakran összemosódik a különféle eszközök és hálózatok magáncélú és céges felhasználása. A mobileszközökön keresztül a céges hálózatok ellen intézett támadás jelentős kockázattal jár a vállalkozásokra nézve. A mobileszközök is számítógépek, és ennek megfelelő védelmet igényelnek.

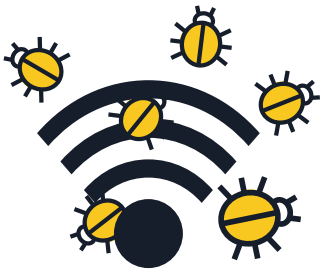


2 Vezessen be a cégnél a saját eszközök használatát szabályozó irányelveket (BYOD)

- A céges adatokhoz és rendszerekhez saját eszközeikkel hozzáférő felhasználóknak a céges irányelvek szerint kell eljárniuk, még akkor is, ha az eszközöket csak levelezésre, naptárkezelésre vagy partnerek adatainak kezelésére használják. Körültekintően válassza ki, hogy a mobileszközök kezeléséhez és védelméhez melyik technológiákat alkalmazzák, és hívja fel a munkatársak figyelmét, hogy legyenek mindig óvatosak.

3 A mobileszközökre vonatkozó biztonsági irányelvek legyenek az átfogó biztonsági keretrendszer részei

- Amennyiben egy eszköz nem felel meg a biztonsági előírásoknak, azt nem szabad a céges hálózathoz csatlakoztatni, ahogyan a céges adatokhoz sem lehet vele hozzáférni. A vállalatoknak érdemes saját mobileszköz-kezelési (MDM) vagy mobilitáskezelési (EMM) megoldásokat bevezetniük.
- Mindezen intézkedések mellett rendkívül fontos egy mobilfenyegetettség ellen védő rendszer telepítése is. Ezzel a megoldással javul a rendszerek átláthatósága, továbbá könnyebben észlelhetővé válnak a különféle alkalmazás-, hálózat- és operációsrendszer-szintű fenyegetések.

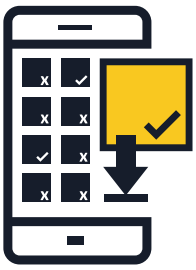


4 Legyen óvatos, ha nyilvános Wi-Fi hálózaton keresztül kíván céges adatokhoz hozzáférni

- Általánosságban elmondható, hogy a nyilvános Wi-Fi hálózatok nem biztonságosak. Ha a cég egyik dolgozója például repülőtér vagy kávézó ingyenes Wi-Fi hálózatán keresztül fér hozzá a céges adatokhoz, azokhoz rosszindulatú felhasználók is hozzáférhetnek. A cégeknek javasolt a „hatékony használatra” vonatkozó irányelvek alkalmazása.

5 Az eszközök operációs rendszere és alkalmazásai legyenek mindig naprakészek

- Javasolja a cég dolgozóinak, hogy telepítsék a mobileszköz operációs rendszerének frissítéseit, amint az eszköz erre vonatkozó üzenetet küld. Különösen az Android rendszerre igaz, hogy érdemes gyakran rákeresni a mobilszolgáltatók és készülékgyártók frissítéseire. A legújabb frissítések telepítésével nemcsak biztonságosabb lesz a készülék, hanem jobban is működik majd.



6 Csak megbízható forrásokból származó alkalmazásokat telepítsen

- A vállalati hálózathoz csatlakozó eszközökre a cég irányelvével összhangban kizárólag hivatalos forrásból származó programok telepíthetők. Hasznos megoldás lehet egy céges alkalmazásbolt kialakítása, ahonnan a felhasználók igény szerint letölthetik az engedélyekkel rendelkező, szükséges alkalmazásokat. A telepítéssel és beállítással kapcsolatban kérje egy biztonsági cég segítségét, vagy hozza létre maga a boltot.

7 Akadályozza meg a szoftvermódosításokat (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. Céges környezetben nem szabad olyan eszközt használni, amelyben engedélyezettek a gyökérműveletek.

8 Fontolja meg a felhőbeli tárolás lehetőségét

- A mobileszközök felhasználóival gyakran előfordul, hogy a fontos dokumentumokhoz nemcsak az asztali gépen, hanem az irodán kívül saját telefonjukon vagy táblagépükön keresztül is szeretnének hozzáférni. Céges szinten érdemes megfontolni a felhőalapú tárolási és fájlszinkronizálási megoldások bevezetését, hogy az ilyen és ehhez hasonló igényeket biztonságos módon lehessen teljesíteni.

9 Kérje meg munkatársait, hogy telepítsenek a mobileszközre biztonsági alkalmazást

- A fertőzés kockázata alól egyik operációs rendszer sem jelent kivételt. Amennyiben lehetséges, a felhasználók mindenképpen használjanak a mobilkészüléken valamilyen biztonsági programot, amely észleli a különféle kémprogramokat és rosszindulatú alkalmazásokat és megakadályozza a településüket, valamint több más, kalózkodás-ellenes és lopásgátló funkcióval rendelkezik.

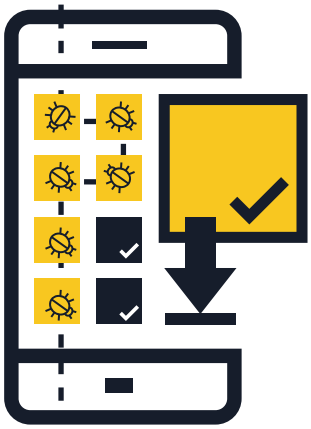
EUROPOL EC3 European Cybercrime Centre | RENDŐRSÉG POLICE | KÉSZENLÉTI RENDŐRSÉG | NEMZETI KIBERVÉDELMI INTÉZET | NMHH Nemzeti Média- és Hírközlési Hatóság | NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

#MobileMalware

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 személyes ne adja meg személyes 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.
- **Ellenőrizze 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 rendszerétől 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 | RENDŐRSÉG POLICE | KÉSZENLÉTI RENDŐRSÉG | NEMZETI KIBERVÉDELMI INTÉZET | NMHH Nemzeti Média- és Hírközlési Hatóság | NISZ NEMZETI INFOKOMMUNIKÁCIÓS SZOLGÁLTATÓ ZRT.

#MobileMalware