



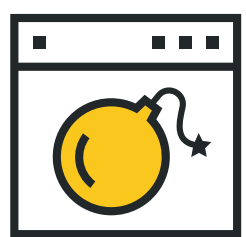
MOBILESZKÖZÖKÖN  
FUTÓ ZSAROLÓVÍRUSOK

# 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 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 weboldakkal, 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.