OUCH! 2021. június

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Mobilalkalmazások biztonságos használata

Áttekintés

Az olyan mobileszközök, mint a tabletek, okostelefonok vagy az okosórák a mindennapi életünk részévé váltak a munkahelyen és a magánéletben egyaránt. Fő vonzerejüket az a sok ezer alkalmazás jelenti, amelyeket általuk használatba vehetünk. Ezek lehetővé teszik, hogy még produktívabbak legyünk, kommunikáljunk másokkal, segítik az oktatást, képzést, vagy egyszerűen csak szórakoztatnak. Az alábbiakban olyan tanácsokat mutatunk be, amelyek segítségével biztonságos módon hozhatjuk ki a legtöbbet a mobileszközök nyújtotta lehetőségekből.

Biztonságos mobilalkalmazások beszerzése

A kiberbűnözők mesterei az olyan rosszindulatú appok létrehozásának, amelyek szakasztott úgy néznek ki, mint az eredetiek. Ha feltelepítünk egy ilyen appot, a bűnözők akár át is vehetik az irányítást eszközünk felett. Éppen ezért fontos meggyőződni arról, hogy csak biztonságos forrásból töltsünk le mobilalkalmazásokat. Sokan nincsenek tisztában azzal, hogy a mobilkészülék márkája alapvetően meghatározza, hogy honnan lehet letölteni appokat.

Apple eszközök esetén például kizárólag az Apple App Store-ból. Előnye, hogy az Apple szigorú biztonsági ellenőrzést végez minden applikáción, mielőtt ezek letölthetővé válnának. Habár az összes káros alkalmazást még így sem lehet kiszűrni, ez a szigorúan ellenőrzött környezet nagyban csökkenti annak kockázatát, hogy rosszindulatú appokat töltsünk le. Továbbá, amennyiben az Apple azonosít egy káros alkalmazást, gyorsan gondoskodik annak eltávolításáról.

Android eszközök esetén csak a Google által működtetett Google Play áruházból töltsünk le applikációkat! Az Apple-höz hasonlóan a Google is biztonsági ellenőrzést végez minden appon, amit elérhetővé tesz a felhasználók számára. A két platform között az alapvető különbség az, hogy androidos készülékeken egyes beállítások lehetőséget adnak arra, hogy más forrásokból is letölthessünk mobilalkalmazásokat. Soha ne éljünk ezekkel a beállításokkal! Az ilyen külső forrásokban ugyanis nagyon könnyű káros appokat elhelyezni, és rávenni a felhasználókat arra, hogy ezeket telepítsék eszközeikre.

Függetlenül attól, hogy milyen típusú készüléket használunk, mindig alaposan nézzünk utána egy appnak, mielőtt azt letöltenénk! Minden esetben ellenőrizzük le, hogy milyen régóta érhető el az alkalmazás, hányan töltötték le, valamint, hogy ki a fejlesztője!

` © SANS Institute 2021

Minél hosszabb ideje érhető el egy alkalmazás, annál több felhasználó próbálhatta ki, és hagyhatott pozitív értékelést. Emellett minél gyakrabban kerül frissítésre egy app, annál valószínűbb, hogy az megbízható. Csak olyan appokat töltsünk le, amelyekre valóban szükségünk van! Egyszerűen kérdezzük meg magunktól: „Egészen biztos, hogy szükségem van erre?” A potenciális sérülékenységek mellett az alkalmazásokat adatvédelmi problémák is érinthetik. Amennyiben egy applikációt már nem használunk, távolítsuk el a készülékünkről! Ha egyszer mégis szükség lenne rá, bármikor újratelepíthetjük.

Adatvédelem és jogosultságok

Ha feltelepítettünk egy alkalmazást, nézzük át az adatvédelmi beállításokat! Biztos, hogy az appnak hozzá kell férnie a helyadatainkhoz, a mikrofonhoz vagy a kontaktjainkhoz? Amikor az alkalmazások számára engedélyezünk egy jogosultságot, azzal az app készítőjének adunk hozzáférést például a földrajzi helyzetünk meghatározásához, vagy épp ahhoz, hogy kereskedjen a rólunk gyűjtött adatokkal. Ha nem szeretnénk megadni a hozzáférést ezekhez az információkhoz, egyszerűen csak utasítsuk el a jogosultságkéréseket, és kizárólag az applikáció használatának idejére engedélyezzük azokat, vagy fontoljuk meg, hogy inkább keresünk egy másik alkalmazást! Ne feledjük, rengeteg alternatíva érhető el.

Az appok frissítése

A mobilalkalmazások, csakúgy, mint a számítógépes programok, folyamatos frissítésre szorulnak. A bűnözők állandóan azon munkálkodnak, hogy az alkalmazásokban újabb és újabb biztonsági hibákat fedezzenek fel, amiket azután kihasználhatnak ellenünk. Az appok fejlesztői pedig azon vannak, hogy biztonsági frissítésekkel mielőbb befoltozzák ezeket a sérülékenységeket. Minél gyakrabban keresünk rá a frissítésekre, és telepítjük azokat, annál jobb! A legtöbb eszköz lehetőséget biztosít ahhoz, hogy az alkalmazások automatikusan frissüljenek. Ez egy erősen javasolt beállítás!

A mobilappok segítségével hozhatjuk ki a legtöbbet eszközeinkből, azonban válasszunk körültekintően, és az alkalmazásokat mindig használjuk biztonságosan!

A szerzőről

Domenica Crognale minőségbiztosítási mérnök, és a SANS Intézet tanúsított oktatója. Emellett az „FOR585: Okostelefon mélyelemzés” kurzus társszerzője. Domenica elérhető a Twitteren @domenicacrognal.

Források:

A frissítés ereje: https://www.sans.org/security-awareness-training/resources/power-updating
Adatvédelem: https://www.sans.org/newsletters/ouch/privacy/
A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)

OUCH! A Sans Security Awareness részleg által közzétett és a Creative Commons BY-NC-ND 4.0 licensz alapján terjesztett hírlevél. A hírlevél szabadon terjeszthető vagy tudatosító programokban felhasználható mindaddig, amíg az nem kerül módosításra. Szerkesztette: Walter Scrivens, Phil Hoffman, Alan Wagoner, Les Ridout, Princess Young.