OUCH! 2024. október

OUCH!

SANS SECURITY AWARENESS

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

A letöltések veszélye: hogyan járj túl a rosszindulatú mobilapplikációk eszén

A titokzatos program: egy rövid figyelemfelhívó mese

Egy lustálkodással és közösségi média görgetéssel töltött vasárnapi napon Sarah egy új fényképszerkesztő appra bukkant, amelynek „PiksPerfect” volt a neve. A program gyönyörű filterei felkeltették a figyelmét, és gondolkodás nélkül letöltötte azt. Eleinte az applikáció remekül működött, de kicsivel később a telefonja egyre lassabbá kezdett válni, és véletlenszerű hirdetések is meg-megjelentek a kijelzőjén. Pár nappal később Sarah-t a bankja kereste fel azzal, hogy több ezer dollárnyi értékű gyanús tranzakció történt a számláján. Ijedtében Sarah megnyitotta bankja applikációját, és azzal szembesült, hogy a megtakarításai majdnem teljes mértékben eltűntek számlájáról. Miután bejelentette a csalást és befagyasztotta számláját, összezavarodva és felzaklatva érezte magát.

Egy informatikában jártas barátja felfedte az igazságot: a mobilapplikáció hamis volt, amely ellopta személyes adatait, beleértve a banki adatait is. Hónapokba telt, mire Sarah felépült, de sokkal elővigyázatosabbá vált: most már minden applikációnak utánanéz, mielőtt letöltené azokat. Manapság már másoknak meséli, hogyan járt, felhívva a figyelmet az elővigyázatosságra, hiszen akár egy pillanatnyi figyelmetlenség is hosszútávú következményekkel járhat.

Honnan tudom, hogy mely appok biztonságosak?

A mobilalkalmazások kényelmesek és sok erőt hordoznak magukban, hiszen szinte bármit képesek vagyunk velük elintézni egy apró gomb megérintésével. Azonban a kiberbűnözők ezt is kihasználják: hamis, vagy éppen rosszindulatú programokat hoznak létre. Ha letöltünk egy ilyen alkalmazást, az képes lehet átvenni az irányítást telefonjaink felett és figyelni minden mozdulatunkat. Védelmünk kulcsa abban rejlik, hogy megbizonyosodjunk róla, hogy a letöltött appjaink valódiak és biztonságosak.

Mindenekelőtt a legfontosabb, hogy csak hivatalos oldalakról szerezzük be alkalmazásainkat, ahol mások is véleményezhették azt, mint például az Apple App Store vagy a Google Play Store. Ezzel csökkenthetjük annak az esélyét, hogy egy rosszindulatú programot töltsünk le. A harmadik személytől származó alkalmazásletöltők gyakran megbízhatatlanok, és tulajdonosaik akár kiberbűnözők is lehetnek. Bár az biztos, hogy akkor is óvatosnak kell lennünk, ha megbízható app store-okat használunk. Itt van néhány plusz tipp, hogy hogyan lehetsz biztos abban, hogy megbízható, biztonságos mobilapplikációkat töltesz le:

1. **Ellenőrizd a fejlesztő nevét**: Amikor egy adott alkalmazást keresel, amit egy adott cég hozott létre, menj biztosra, hogy azt az alkalmazást töltöd le, amit az a cég fejlesztett! A csalók egyik gyakori trükkje az, hogy olyan appokat hoznak létre, amik nagyon hasonlítanak az ismert társaikhoz. Ellenőrizd a fejlesztő nevét - ugyanaz a cég vagy ismert fejlesztő, akiről tudsz, vagy valaki olyan készítette, akiről sohasem hallottál? Felkeresheted akár a program vagy maga a fejlesztő hivatalos weboldalát, hogy felleld a direkt linkeket az appokhoz az app store-ban. Ezzel megbizonyosodhatsz arról, hogy az eredeti applikációt töltöd le.

2. **Olvasd el a véleményeket és értékeléseket**: Olvasd át a felhasználók véleményeit és értékeléseit! Egy hivatalos alkalmazásnak jelentős mennyiségű pozitív hozzászólása és magas értékelései vannak. Óvakodj azoktól, amelyekhez kevesen szóltak hozzá, vagy negatívan véleményeztek, vagy éppen ellenkezőleg, túlságosan pozitív benyomást keltenek: már annyira, hogy megkérdőjelezed a valódiságát!

3. **Ellenőrizd a letöltések számát**: A valós applikációknál általában magas a letöltések száma. Egy kevés letöltési számmal rendelkező applikáció viszont intő jel lehet.

4. **Ellenőrizd a hozzáférési engedélyeket**: Letöltés előtt mindig ellenőrizd, hogy milyen hozzáférési engedélyeket kér az alkalmazás! Alapesetben egy alkalmazás csak olyan funkciókhoz kér hozzáférést, amelyek elengedhetetlenek a működéséhez. Légy óvatos azokkal, amelyek sok és nem releváns hozzáférésre akarnak minket rávenni. Példának okáért: biztos, hogy az appnak mindig hozzá kell férnie a geolokációnkhoz,- vagy kontaktjainkhoz?

5. **Frissíts rendszeresen**: A valós alkalmazásokat rendszeresen frissítik, hogy kijavítsák a hibáikat és növeljék a teljesítményüket. Ellenőrizd az app frissítési előzményeit és győződj meg róla, hogy gyakran frissítik-e!

6. **Légy óvatos az új mobilalkalmazásokkal**: Érdemes kellő elővigyázatossággal kezelni azokat az új applikációkat, amelyekkel kapcsolatban még nem érkezett vélemény sem pedig értékelés. Ha valós, akkor csak idő kérdése, mire pozitív megítélést és értékelést kap.

Ha letöltöttél egy mobilapplikációt, engedélyezd az automatikus frissítést! Mindig találni új hibákat és sérülékenységeket ezek kódjaiban és konfigurációiban. Azzal, hogy biztosítod, hogy mindig a legutóbbi verzióját futtatod az alkalmazásaidnak, megbizonyosodhatsz róla, hogy ezek a sérülékenységek javításra kerülnek és a legújabb biztonsági funkciókkal rendelkezel. Ugyanakkor: ha már nem használsz, vagy nincs szükséged egy adott mobilapplikációra, a legjobb az, ha letörlöd a készülékedről.

A szerzőről

Danielle Strimbu technológiai illetve operációs management háttérrel rendelkezik, jelenleg technikai projektmenedzser a Travel Minds Digital Agency-nél. Mint a WiCyS Colorado Affiliate rendezvényelnöke, célja olyan események létrehozása, amely segíti a nőket a kiberbiztonság területén való előre lépésben. Kiberbiztonság Management alapdiplomával és Információs Rendszerek Biztonsága mesterdiplomával rendelkezik.

Források

Top három módszer, ahogy a (Kiber)támadók célpontjává válunk: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
Érzelmi triggerek – Így csapnak be minket a kibertámadók: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
All You Need to Know About Background Data: https://www.avast.com/c-what-is-background-data#

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)