Hogyan használjuk biztonságosan okostelefonunkat?

Sajtóközlemény – 2020.01. /PResston PR

Manapság az okostelefonok jóformán mindenki zsebében ott lapulnak. Sokszor nem is gondolunk bele, hogy egy olyan eszköz, ami már a mindennapjaink része, akár veszélyforrás is lehet az életünkben. Mik azok az óvintézkedések, amiket érdemes betartani a saját biztonságunk, illetve készülékünk védelme érdekében?

Hitelesítés

Azt gondolnánk, hogy a telefonunk lezárása magától értetődő dolog, ám a közhiedelemmel ellentétben nem mindenki védi okostelefonját hitelesítési intézkedésekkel, ami hatalmas veszélyt hozhat ránk. Ha netán elveszítjük vagy ellopják az okostelefonunkat, rövid idő alatt illetéktelen személy férhet hozzá a levelezésünkhöz, egyéb személyes fiókjainkhoz, továbbá bizalmas adataink, fotóink is rossz kezekbe kerülhetnek. Ezért nagyon fontos, hogy mindig zárjuk le biztonságosan készülékünket! Amikor azt mondjuk, hogy „biztonságosan", akkor nem arra kell gondolni, hogy egy „L" alakú mintát rajzolunk, vagy az 1234-et választjuk PIN-kódnak. A legjobb az, ha biometrikus funkciót *is* használunk (pl. ujjlenyomat vagy arcfelismerés) a jelszó mellett.

A hivatalos áruház használata

Akármennyire is csábítóan hangzik, hogy készülékünket rootoljuk vagy más módon feltörjük, a legtöbb gyártó erről erősen lebeszél bennünket. Az ilyen típusú beavatkozások eredményeképpen eszközünket szükségtelen kockázatoknak tesszük ki, mert előfordulhat, hogy a rootolás következtében a készülékünkön megjelennek nem hivatalos alkalmazásboltok is, amelyeket nem ellenőriznek olyan szigorúan, mint a hivatalos verziókat. Ez akár ahhoz is vezethet, hogy rosszindulatú alkalmazásokat töltünk le, amelyek hatalmas pusztítást okozhatnak az eszközünkön. A kockázatok minimalizálása érdekében a legjobb a hivatalos boltoknál maradni.

Alkalmazások engedélyezése

Az alkalmazások különféle engedélyeket szoktak kérni, hogy megfelelően működhessenek. De legyünk őszinték! Általában csak figyelmetlenül tovább görgetjük

az engedélykérés hosszú leírását, és már nyomunk is az „elfogadom" gombra. Bármilyen kényelmes is lehet ez a módszer, azért mindig fussunk gyorsan végig az alkalmazás által kért engedélyek listáján. Ha mindent elfogadunk gondolkodás nélkül, akkor lehet, hogy ezzel hozzáférést biztosítunk a csalóknak az érzékeny adatainkhoz, vagy lehetővé tesszük számukra, hogy pénzt csaljanak ki tőlünk, vagy kémkedjenek utánunk. Gondoljuk csak végig: egy zseblámpa-alkalmazásnak valóban szükséges hozzáférést biztosítanunk a mikrofonhoz vagy a kamerához?

Biztonsági szoftver használata

A legtöbb ember alábecsüli az okostelefonok védelmére szolgáló biztonsági szoftverek használatának fontosságát. Ennek oka talán az, hogy még mindig inkább telefonnak tekintik az okostelefont, nem pedig zsebben hordható személyi számítógépnek. A tapasztalatok azonban azt mutatják, hogy az okostelefonokra hasonló veszélyek leselkednek, mint a számítógépekre, hiszen a mobil eszközeink is válhatnak vírustámadás áldozatává, vagy akár illetéktelenek férhetnek hozzá a kameráikhoz. Ezért ne feledkezzünk meg arról, hogy a jó hírű, minőségi biztonsági szoftverek megkímélhetnek bennünket ettől a fejfájástól, ugyanis védelmet nyújtanak a kiberfenyegetések és trójai fertőzések ellen, mindemellett biztosítják érzékeny adatainak védelmét, és segítséget nyújtanak az elveszett vagy ellopott eszközök megtalálásában is. Hogyha szeretnénk kipróbálni egy megbízható vírusírtó programot, akkor most az AV-Comparatives tesztjén két arany és egy bronz díjat szerzett ESET ajánlata Nekünk szól. A promóció keretein belül most az ESET Mobile Security ingyenes verziójának letöltése mellett, 30 napig elérhetjük a prémium funkciókat is, amely olyan hasznos védelmi programokat tartalmaz mint például a Lopásvédelem vagy az Adathalászat elleni védelem.

Link:…….

Távoli törlés

Az előző tipphez kapcsolódóan meg kell említeni, hogy az elismertebb biztonsági szoftverek szolgáltatói elérhetővé teszik az úgynevezett távoli törlés opciót is. Ez egy drasztikus megoldás, amivel természetesen senki nem szeretne élni, de adott esetben szükség lehet rá, ugyanis segítségével távolról törölhetjük az elveszett vagy ellopott eszközön lévő adatokat. Bár radikális megoldásnak tűnhet, szerencsés, ha

rendelkezésünkre áll abban az esetben, ha bizalmas vagy érzékeny adatokat tárolunk elveszett készülékünkön. Alternatív megoldásként úgy is beállíthatjuk az eszközünket, hogy az törölje a készüléken hozzáférhető adatokat, amennyiben a hitelesítés magadott számú alkalommal sikertelen volt.

Titkosítás, biztonsági mentés és javítások

Az egyik szabály, amelyet mindenkinek mindig be kellene tartania, az, hogy biztonsági másolatot készítsen adatairól. Abban az esetben, ha olyan rosszindulatú támadás áldozatává válunk, amely megrongálhatja vagy lezárhatja a fájljainkat, akkor legalább rendelkezésünkre áll majd egy biztonsági másolat, amelyet a helyreállításhoz használhatunk. A fájlok titkosítása szintén egy olyan kritikus lépés, amelyet nem szabad alábecsülni. Ilyenkor vehetjük hasznát egy "hagyományos" titkosító programnak, amelynek segítségével pillanatok alatt megoldható a fájlok titkosítása. A kockázatok csökkentése érdekében mindig telepítsük a készülékünkre a legfrissebb hivatalos frissítéseket, mivel azok gyakran tartalmaznak biztonsági javításokat, amelyek segítenek a védekezésben.

Hogyan adjunk túl telefonunkon biztonságosan

Ha túl akarunk adni telefonunkon, akkor több dolgot is szükséges elintéznünk, mielőtt kiadjuk a kezünkből a készüléket. Az eszköztől függően ez magában foglalhatja a meghajtó titkosítását, majd törlését, illetve azt, hogy kijelentkezünk az összes általunk használt szolgáltatásból. Ezzel biztosíthatjuk, hogy személyes adataink továbbra is sértetlenek maradjanak.

Átverős hívások és adathalász SMS-ek

Az adathalász csalások sokféle formában léteznek, és bár az e-mail a legnépszerűbb csatorna, messze nem ez az egyetlen. Például kaphatunk, fertőzött linkeket tartalmazó SMS-eket is, amelyek rosszindulatú szoftvert tartalmazhatnak. A közelmúltban az is előfordult, hogy nemzetközi számokról hívták fel az áldozatokat – olyan országokból, amelyekkel a hívott félnek soha nem volt eddig kapcsolata. Ha visszahívjuk a számot, egetverő költségeket verhetnek ránk. Kétszer is gondoljuk meg, hogy visszahívunk-e külföldi, ismeretlen számokat.

Velünk nem történhet meg?

Remélhetőleg soha nem kell majd foglalkoznunk olyan gondokkal, mint egy biztonsági sérülés vagy netán a fiókjaink feltörése. De ha felismerjük, hogy a veszély mindig fennáll, hosszú távon jobban járunk, mert minimálisra csökkenthetjük a károkat. A biztonsági mentések, a vírusvédelem és a telefon lezárása mellett fontos, hogy az eszköz a távolból is törölhető legyen. Ha megfogadjuk ezeket a tanácsokat, készen állunk majd arra, hogy megfelelően kezeljük a váratlan helyzetet.

A Sicontact Kft.-ről röviden:

A Sicontact Kft. hazánkban az egyik legjelentősebb **IT biztonsággal foglalkozó** cég, az ESET termékek kizárólagos magyarországi forgalmazója. Mottója és küldetése, ami köré termékportfolióját kialakította: „**biztonság a digitális világban**". A Sicontact Kft. Magyarországon az **ESET NOD32** technológiára épülő termékeivel mind a lakossági, mind a vállalati szegmensben meghatározó piaci szereplő. A cég 2007-ben megszerezte az ESET ausztriai képviseletét, így azóta regionális piaci szereplőként tevékenykedik. A Sicontact Kft. több ízben elnyerte a kitüntető **Business Superbrands** díjat. Az ESET Smart Security programcsomagot többször is **az év antivírus megoldásának** választották.

A független tesztelő szervezet több díjjal is elismerte az otthoni ESET termékeket a 2019-es eredményeket összefoglaló riportjában:

- Arany díjat nyert a fejlett, célzott és fájlnélküli kártevő támadások kivédésében, amely új kategóriaként jelent meg 2019-ben. Az ESET volt azon két gyártó egyike, akik mind a 15 célzott támadást sikeresen blokkolták a tesztelés során.

- 2018-ban ezüst, majd 2019-ben arany díjat szerzett a rendszer gyorsaságára és teljesítményére gyakorolt hatást vizsgáló kategóriában, az ESET szoftverek alacsony erőforrásigényének köszönhetően.

- Bronz díjat nyertek el a téves riasztások kategóriájában, amelyek ugyanúgy gondot okozhatnak, mint egy valós fertőzés, ezért az elkerülésük kulcsfontosságú a biztonsági szoftvereknél.

A Sicontact Kft. az ESET szoftvereit a lehető legrugalmasabb konstrukciókban, magyar nyelvű terméktámogatással kínálja. Az ESET már több mint 25 éve biztosít védelmet a digitális világ fenyegetéseivel szemben. Egy kicsi és dinamikus vállalatból mára egy több mint 100 millió felhasználót számláló és 202 országot és területet lefedő globális márkává nőtte ki magát. Rengeteg minden változott, de az alapvető törekvéseik és a hozzáállásuk változatlan maradt,

továbbra is céljuk egy biztonságosabb digitális világ felépítése, amelyben mindenki élvezheti a biztonságos technológia előnyeit.

További információ és interjúegyeztetés:

Terdik Adrienne | **Ügyvezető igazgató | PResston PR | Rózsadomb Center | 1025 Budapest | Törökvész u. 87-91. | T + 36 1 325 94 88 | F +36 1 325 94 89 | M +36 30 257 60 08 | adrienne.terdik@presstonpr.hu | www.presstonpr.hu**

Szekeres Nikoletta | PR tanácsadó | PResston PR | Rózsadomb Center | 1025 Budapest | Törökvész u. 87-91. | T + 36 1 325 94 88 | F +36 1 325 94 89 | M +36 30 831 64 56 | nikoletta.szekeres@presstonpr.hu | www.presstonpr.hu