Vaš mesečni bilten za podizanje svesti o bezbednosti informacija

Bezbedno korišćenje mobilnih aplikacija

Uvod

Mobilni uređaji poput tableta, pametnih telefona i satova postali su jedna od osnovnih tehnologija koju koristimo kako u privatnom tako i u profesionalnom životu. Ono što mobilne uređaje čini tako posebnim jesu milioni aplikacija koje za njih imamo na raspolaganju. Ove aplikacije nam omogućavaju da budemo produktivniji, brže komuniciramo i razmenjujemo informacije sa drugima, da učimo i obrazujemo se ili samo da se više zabavljamo. U nastavku vam predstavljamo korake koje možete preduzeti kako biste vaše mobilne aplikacije koristili na bezbedan način.

Preuzimanje bezbednih mobilnih aplikacija

Sajber kriminalci su ovladali veštinama izrade i distribuiranja zlonamernih mobilnih aplikacija koje izgledaju kao da su legitimne. Ako instalirate neku od tih aplikacija, kriminalci mogu da u potpunosti preuzmu kontrolu nad vašim mobilnim uređajem ili podacima. Zbog toga je potrebno da aplikacije preuzimate samo sa dobro poznatih, pouzdanih izvora. Ono čega možda niste svesni je da brend mobilnog uređaja koji koristite određuje vaše opcije za preuzimanje aplikacija.

Mobilne aplikacije za Apple uređaje preuzimajte samo iz zvanične Apple-ove prodavnice (Apple App Store). Prednost ovoga je što Apple radi bezbednosnu proveru svih mobilnih aplikacija pre nego što ih učini dostupnim za preuzimanje. Iako Apple ne može da otkrije sve maliciozne mobilne aplikacije, ovakvo kontrolisano okruženje značajno smanjuje rizik od instalacije zlonamerne aplikacije. Pored toga, ako Apple u svojoj prodavnici pronađe aplikaciju za koju utvrdi da je maliciozna, brzo će je ukloniti.

Mobilne aplikacije za Android uređaje preuzimajte samo iz zvanične prodavnice Google Play, koju održava Google. Slično kao Apple, Google radi bezbednosnu proveru svih aplikacija pre nego što ih učini dostupnim korisnicima. Razlika kod Android uređaja je što na njima možete da konfigurišete određene opcije kako bi vam bilo omogućeno da preuzimate mobilne aplikacije i iz drugih izvora. Upozoravamo vas da to ne činite, jer svako, uključujući sajber kriminalce, može lako da kreira i distribuira zlonamerne mobilne aplikacije i prevari vas da zarazite svoj mobilni uređaj.
Ma koji brend mobilnog uređaja da koristite, istražite aplikaciju pre nego što je preuzmete. Proverite koliko dugo je aplikacija dostupna, koliko ljudi je koristi i ko je njen proizvođač.
Što je duže aplikacija javno dostupna, što je više ljudi koji su je koristili i ostavili pozitivne komentare o njoj, što je češće proizvođač ažurira, to je veća verovatnoća da se aplikacija može smatrati bezbednom. Pored toga, instalirajte samo one aplikacije koje su vam neophodne i koje koristite.

Zapitajte se, da li vam je aplikacija koju razmišljate da instalirate zaista neophodna? Ne samo da svaka aplikacija potencijalno donosi nove ranjivosti, već ona nosi i nove teme i probleme u vezi sa privatnošću. Ako prestanete da koristite aplikaciju ili je više ne smatrate korisnom, uklonite je sa svog mobilnog uređaja (uvek je možete instalirati kasnije ako vam bude zaista potrebna).

Privatnost i dozvole u aplikacijama

Prilikom instalacije mobilne aplikacije osigurajte da ona bude bezbedno podešena i da štiti vašu privatnost. Da li mobilna aplikacija zaista treba da ima pristup vašoj lokaciji, mikrofonu ili kontaktima? Ako date tražene dozvole, time možete omogućiti kreatoru aplikacije da vas prati, pa čak i da sa drugima razmenjuje ili da im proda vaše informacije. Ako ne želite da date tražene dozvole, jednostavno odbijte zahtev koji vam je aplikacija postavlja. Dajte samo one dozvole za koje ste sigurni da ih aplikacija opravdano koristi. Uvek možete potražiti drugu aplikaciju koja zadovoljava vaše potrebe i ne zahteva preširoke dozvole. Zapamtite, imate puno drugih aplikacija na raspolaganju.

Ažuriranje aplikacija

Mobilne aplikacije, baš kao i vaš računar i operativni sistem mobilnog uređaja, moraju da se ažuriraju da bi bile bezbedne. Kriminalci neprestano traže i pronalaze slabosti u aplikacijama, a potom razvijaju načine za eksploataciju ovih ranjivosti. Programeri koji su kreirali vašu aplikaciju takođe kreiraju i objavljuju ažuriranja kako bi ispravili ove ranjivosti i zaštitili vaše uređaje. Što češće proveravate i instalirate ažuriranja, to bolje. Većina uređaja vam omogućava da konfigurišete sistem tako da se mobilne aplikacije ažuriraju automatski. Preporučujemo vam da to i učinite.

Mobilne aplikacije omogućavaju da vaše uređaje koristite na najbolji mogući način. Budite pažljivi kod odabira aplikacija i pobrinite se da ih koristite na bezbedan način.

Gost urednik

Domenika Krognejl je inženjer za osiguranje kvaliteta i sertifikovani instruktor SANS instituta. Jedan je od autora obuke FOR585: Smartphone Analysis In-Depth. Na Tviteru je možete pronaći kao @domenicacrognal.

Dodatni materijal

Moć ažuriranja: https://www.sans.org/newsletters/ouch/the-power-of-updating/
Privatnost - zaštitite vaše digitalne tragove: https://www.sans.org/newsletters/ouch/privacy/

Preveli za zajednicu: Dragan Ristić i Gordana Živanović