Kako da zaštitite vaše mobilne uređaje

Uvod

Mobilni uređaji omogućavaju veoma jednostavnu komunikaciju sa prijateljima, kupovinu putem interneta, pristup mobilnom bankarstvu, gledanje filmova, igranje igrica i obavljanje brojnih drugih aktivnosti. Kako njihovo korišćenje čini važan deo vaših života, od velike je važnosti da i vi i vaši uređaji ostanete bezbedni.

Zaštitite vaše uređaje

Možda će vas iznenaditi činjenica da najveći rizik po vaše mobilne uređaje ne predstavljaju hakeri, već najverovatnije vi sami. Mnogo je veća verovatnoća da ćete izgubiti ili zaboraviti svoj mobilni uređaj nego da će ga neko hakovati. Prvo što u cilju zaštite treba da preduzmete je da omogućite automatsko zaključavanje ekrana kada se uređaj ne koristi. To znači da, kada hoćete da koristite vaš mobilni uređaj, moraćete prvo da otključate ekran korišćenjem jake lozinke, PIN-a, prepoznavanja lica ili otiska prsta. Ovim se u značajnoj meri onemogućava da neko drugi pristupi vašim informacijama ako uređaj bude izgubljen ili ukraden. Dodatno, omogućavanje zaključavanja ekrana na većini mobilnih uređaja uključuje i enkripciju, što doprinosi zaštiti podataka koji se čuvaju na uređaju.

Dodatni saveti koji će vam pomoći da zaštitite vaše uređaje su sledeći:

1. **Ažuriranje**: Uključite automatsko ažuriranje na vašim uređajima jer time obezbeđujete da oni uvek koriste najnovije verzije operativnog sistema i aplikacija. Sajber kriminalci neprestano traže nove ranjivosti u softveru, a proizvođači stalno objavljuju nove verzije i ispravke kako bi ih što pre otklonili. Kada uređaje držite ažurnim, značajno otežavate njihovo hakovanje. Prilikom izbora novog Android uređaja, proučite i obaveze proizvođača u pogledu ažuriranja uređaja. Apple iOS uređaje ažurira sama kompanija, dok Android mobilne uređaje ažuriraju pojedinačni proizvođači, koji nisu podjednako posvećeni njihovom ažuriranju. Ako koristite stari uređaj koji više nije podržan ili ga nije moguće ažurirati, razmotrite kupovinu novog.

2. **Praćenje**: Instalirajte ili omogućite softveru kome verujete da udaljeno prati vaš mobilni uređaj preko interneta. Tako ćete, u slučaju da uređaj bude izgubljen ili ukraden, imati mogućnost da se preko interneta povežete sa njim i saznate lokaciju, a u najgorem slučaju i da udaljeno obrišete sve vaše informacije.

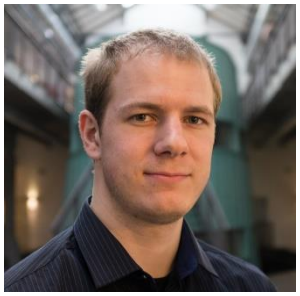
3. **Mobilne aplikacije od poverenja**: Instalirajte samo aplikacije koje su vam neophodne i držite se pouzdanih izvora. Za Apple iOS uređaje, kao što su iPad i iPhone, to znači da aplikacije treba da preuzimate sa Apple App Store-a. Za Android uređaje preuzimajte aplikacije sa Google Play-a, a za Amazon tablete sa Amazon App Store-a. Iako aplikacije možete da preuzimate i sa drugih sajtova, znajte da one nisu proverene i veća je verovatnoća da budu zaražene ili zlonamerne, što može ugroziti vašu privatnost. Takođe, pre nego što preuzmete aplikaciju, uverite se da ona ima veliki broj pozitivnih komentara i da je proizvođač često ažurira. Izbegavajte potpuno nove aplikacije, aplikacije sa svega nekoliko komentara ili one koje se retko ažuriraju.

4. **Podešavanja privatnosti**: Mobilni uređaji prikupljaju opsežne informacije o vama, posebno jer ih nosite svuda gde se krećete. Pažljivo pregledajte podešavanja privatnosti uređaja, uključujući i praćenje lokacije, i uverite se da se osetljiva obaveštenja (poput verifikacionih kodova) ne pojavljuju na ekranu kada je uređaj zaključan.

5. **Posao**: Uvek prethodno proverite da li su mobilni uređaji koje nameravate da koristite za poslovne aktivnosti odobreni od strane vašeg poslodavca. Kada ste na poslu, budite posebno oprezni i nikada ne fotografišite i ne snimajte bilo šta što bi moglo da sadrži osetljive informacije, poput skica sa tabli ili prikaza na ekranu računara.

Mobilni uređaji su moćni alati koje želimo da koristimo i u tome uživamo. Primenom ovih nekoliko jednostavnih koraka možete učiniti mnogo u pogledu sopstvene zaštite i zaštite vaših uređaja.

Gost urednik



Jeroen Bekers je ekspert za bezbednost mobilnih uređaja u kompaniji NVISO, koautor OWASP MASVS smernica i MSTG uputstva, instruktor SANS instituta i autor kursa SEC575: Mobile Device Security and Ethical hacking. Možete ga pronaći putem LinkedIn-a na https://www.linkedin.com/in/beckersjeroen/.

Dodatni materijal

Moć ažuriranja: https://www.sans.org/newsletters/ouch/the-power-of-updating
Bezbedno korišćenje mobilnih aplikacija: https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/
Napadi putem tekstualnih poruka: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks
Napravite lozinku na jednostavan način: https://www.sans.org/newsletters/ouch/making-passwords-simple
Telefonski napadi i prevare (višing): https://www.sans.org/newsletters/ouch/vishing

Preveli za zajednicu: Dragan Ristić i Gordana Živanović