Mesečni bilten bezbednosnih saveta za korisnike računara

OUCH!

U OVOM IZDANJU...

- **Kako da obezbedite svoj novi tablet**
- **Kako da ostane bezbedan**

Bezbednost vašeg novog tableta

Uvod

Sve čestitke na vašem novom tabletu, tehnologiji koja već nekoliko godina unazad predstavlja moćan praktičan način za komunikaciju sa drugima, on-line kupovinu, gledanje filmova, igranje igara i obavljanje bezbroj drugih aktivnosti. Pošto će vaš novi teblet najverovatnije postati važan deo vašeg života, možda čak i zameni vaš računar, predstavićemo vam nekoliko ključnih smernica koje treba primeniti da bi vaš tablet i vaše informacije bile bezbedne.

Gost urednik

Lori Rosenberg ima veliko iskustvo u kreiranju edukacionog materijala iz oblasti bezbednosti informacija i obuke korisnika i klijenata. Veoma je posvećena u pronalaženju novih, zanimljivijih metoda prenošenja znanja. Možete je pratiti na Twitter-u na **@InfoSecLori**.

Kako da obezbedite svoj novi tablet

Možda vas iznenadi činjenica da najveći rizik za vaš tablet ne predstavljaju hakeri ili sajber kriminalci, već vi sami. Daleko je veća verovatnoća da će te svoj tablet izgubiti, zaboraviti negde ili da će vam ga neko ukrasti, nego da će ga neko hakovati. Prvu stvar koju je potrebno da uradite da bi ste obezbedili svoj tablet je da aktivirate automatsko zaključavanje ekrana jakom, pouzdanom lozinkom, uzorkom za prevlačenje ili otiskom prsta. Tako ćete osigurati da čak i kada je vaš tablet izgubljen ili ukraden niko ne može da mu pristupi, i da su vaše informacije, aplikacije i sve ostalo na njemu zaštićeni. Kada ste aktivirali automatsko zaključavanje ekrana, uzmite u obzir i sledeće savete:

1. Instalirajte i aktivirajte softver za daljinsko praćenje tableta preko Interneta. Na taj način ćete, ako je tablet izgubljen ili ukraden, biti u mogućnosti da se povežete na njega preko Interneta i da otkrijete njegovu lokaciju, ili u najgorem slučaju da daljinski obrišete sve svoje informacije.
2. Ažurirajate svoj tablet i aktivirajte automatsko ažuriranje tako da uvek funkcioniše sa najnovijom verzijom operativnog sistema. Sajber kriminalci su uvek u potrazi za neotkrivenim softverskim propustima i greškama, a proizvođači konstantno objavljuju nove ispravke i zakrpe. Korišćenjem najnovijih verzija operativnog sistema i aplikacija, u mnogome otežavate nekom da kompromituje vaš uređaj.
3. Budite veoma obazrivi kada prvi put konfigurišete svoj tablet, posebno sa postavkama vezanim za privatnost. Jedna od najbitnijih stavki vezanih za privatnost je svakako mogućnost drugih da prate vašu lokaciju. Naša je preporuka

Bezbednost vašeg novog tableta

da inicijalno onemogućite praćenje lokacija, a da je nakon toga aktivirate samo za aplikacije za koje mislite da treba da imaju tu mogućnost. Za neke aplikacije je ta mogućnost važna i neophodna, na primer za mape ili pronalaženje lokalnih restorana, ali je za većinu aplikacija informacija o vašoj trenutnoj lokaciji nepotrebna.

4. Većina tableta i samih aplikacija skladište korisničke informacije u računarskom oblaku (Cloud), tako da je bitno da razumete gde se vaši podaci uskladišteni i kako su obezbeđeni. Na primer, sigurno ne želite da vam se dogodi da vaše privatne fotografije, zajedno sa geolokacijskim informacijama o njima, budu dostupne svima na Internetu. Inicijalnim podešavanjem isključite svako deljenje informacija u „cloud“ servisima, a onda aktivirajte deljenje samo za specifične stvari za koje ste sigurni da želite da podelite sa drugima.

Najbolji način da obezbedite svoj tablet je da aktivirate zaključavanje ekrana, proverite podešavanja vezana za privatnost i redovno ga ažurirate.

5. Tableti takođe imaju mogućnost da sinhronizuju aplikacija sa drugim uređajima, na primer sa vaši pametni telefonom ili laptopom. Sinhronizacija može da bude veoma korisna osobina, ali uvek budite oprezni kako i šta dozvoljavate da se sinhronizuje. Ako vam je sinhronizacija uvek i bez izuzetka aktivirana, nemojte biti iznenađeni ako se celokupna istorija Internet pretrage i tabova koje ste kreirali na pretraživaču vašeg tableta u jednom momentu pojavi u Internet pretraživaču računara koji koristite na poslu.

Kako da ostane bezbedan

Kada ste jednom obezbedili svoj tablet, svakako želite i da tako ostane. Da bi ste na duži vremenski period osigurali bezbednost svog tableta, sledite sledeće savete:

- Nikada nemojte narušavati sistemske privilegije fabrički podešene (jailbreak-ovanje ili root-ovanje). Takvim postupcima ćete zaobići i obezvrediti veliki broj ugrađenih bezbednosnih kontrola i učiniti svoj tablet mnogo ranjivijim na sajber napade.
- Preuzimajte samo aplikacije koje su vam potrebne i uvek iz pouzdanih izvora. Za iPad-e, samo iz iTune-a. Te aplikacije su provere od strane Apple-a pre negu su postale dostupne korisnicima. Za Android uređaje preporučujemo da uvek preuzimate aplikacije iz Google Play-a i za Amazon tablete samo iz Amazon App Store-a. Mada aplikacije

Bezbednost vašeg novog tableta

možete preuzeti i sa drugih Internet stranica, to nije preporučljivo obzirom da nema garancija da su aplikacije proverene i da neće inficirati vaš uređaj. Na kraju, bez obzira kako ste preuzeli neku aplikaciju, kada vam više nije potrebna ili je ne koristite aktivno, preporučljivo je da je uklonite (deinstalirate).

- Kada instalirate novu aplikaciju, budite sigurni da ste proverili podešavanja vezana za privatnost, na isti način kako ste to uradili prilikom inicijalnog podešavanja vašeg tableta. Budite oprezni u vezi dozvola za pristup podacima svake aplikacije. Na primer, da li aplikacija koju ste preuzeli stvarno treba pristup informacijama o vašim kontaktima ili prijateljima? Ako niste zadovolji zahtevima za pristup informacijama određene aplikacije, nađite neku drugu koja vam više odgovara. Pored toga, redovno proveravajte dozvole za pristup da bi ste bili sigurni da u međuvremenu nisu promenjene ili poremećene.

Tablet je moćna alatka koja vam, ako se koristi na ispravan i bezbedan način, može pružiti veliko zadovoljstvo i korist. Uvek imajte na umu da ako pravilno primenite i pridržavate se navedenih saveta, osiguraćete ne samo svoj uređaj nego i svoje podatke, što je često mnogu bitnije.

Saznaj Više

Prijavi se na OUCH! mesečni bilten bezbednosnih saveta za korisnike računara, pristupi prethodnim OUCH! izdanjima i saznaj više o SANS rešenjima u vezi svesnosti bezbednosti informacija na našoj internet prezentaciji http://www.securingthehuman.org.

Dodatne informacije

Bezbedno korišćenje aplikacija na mobilnim uređajima:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201501_se.pdf
Propusne fraze:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_se.pdf
Bezbedno korišćenje računarskog oblaka:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201409_se.pdf
Rashodovanje mobilnih uređaja:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201406_se.pdf
Tip dana:	https://www.sans.org/tip_of_the_day.php

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Preveo: Nenad Varinac