SANS Telekom Srbija

OUCH! | Oktobar 2017

Mesečni bilten za podizanje svesti o bezbednosti informacija

OUCH!

U OVOM BROJU...

Pomozite drugima da budu bezbedni

Uvod

Mnogi od nas su sa tehnologijom “na ti”, uključujući i njeno bezbedno korišćenje. To često nije slučaj sa nekim našim prijateljima ili rođacima. Oni zapravo mogu biti zbunjeni, zastrašeni ili čak uplašeni, što ih čini veoma ranjivim na savremene sajber napade. Sajber bezbednost ne treba da plaši, jer je zapravo prilično jednostavna kada se jednom shvate osnovni principi. Njima je najverovatnije samo potreban vodič, poput vas samih, da im pomogne da razumeju najosnovnije.

Gost urednik

Rendi Markejni (Twitter: **@randymarchany**) je rukovodilac informacione bezbednosti na Univerzitetu Virdžinija Tek i sertifikovani instruktor SANS instituta.

Pet jednostavnih koraka

U nastavku je pet jednostavnih koraka koje možete preduzeti da pomognete drugima da prevaziđu strahove i na bezbedan način maksimalno iskoriste tehnologije. Više informacija o svakom od ovih koraka možete dobiti u delu Dodatne informacije na kraju ovog biltena.

1. **Socijalni inženjering**: Socijalni inženjering je tehnika koju često koriste sajber kriminalci kako bi prevarili ljude i naveli ih da urade nešto što ne bi trebalo, kao na primer da odaju svoju lozinku, zaraze svoj računar malverom ili otkriju osetljive informacije. Ova tehnika ne predstavlja ništa novo, jer prevaranti postoje hiljadama godina unazad. Jedina razlika je u tome što loši momci sada te iste metode primenjuju na Internetu. Možete pomoći drugima tako što ćete im objasniti najčešće znake napada, na primer kada neko pokušava da stvori utisak hitnosti, kada je nešto suviše dobro da bi bilo istinito, ili kada se napadač pretvara da je neko koga osoba poznaje ali njegove poruke ne deluju kao da ih je taj neko napisao. Upoznajte ih sa primerima najčešćih napada, kao što je sajber pecanje (phishing) putem elektronske pošte ili telefonski pozivi od strane lažne Microsoft tehničke podrške. Ako ništa drugo, uverite se da razumeju da ne smeju nikome da odaju svoju lozinku niti dozvole udaljeni pristup svom računaru.
2. **Lozinke**: Jake lozinke su ključne za zaštitu uređaja i naloga na Internetu. Podučite druge kako da kreiraju jake lozinke. Mi preporučujemo korišćenje fraza, jer ih je najlakše otkucati i zapamtiti. Fraze su ništa drugo nego lozinke koje se sastoje od više reči. Pored toga, pomozite im da instaliraju i koriste menadžera lozinki. Važno je imati jedinstvenu lozinku za svaki vaš uređaj i nalog. Ako je korišćenje menadžera lozinki za njih suviše komplikovano, posavetujte ih možda

Pomozite drugima da budu bezbedni

da svoje lozinke zapišu i čuvaju na bezbednom mestu. Na kraju, pomozite im da za važne naloge omoguće verifikaciju iz dva koraka (poznatu i kao dvofaktorska autentifikacija). Verifikacija iz dva koraka je jedan od najefikasnijih koraka za zaštitu ma kojeg naloga.

3. **Primena ispravki**: Održavanje sistema ažurnim i primena svih ispravki je ključni korak koji svako može da preduzme kako bi obezbedio svoje uređaje. Ovo ne važi samo za vaše računare i mobilne uređaje, već za sve što je povezano na Internet, poput konzola za igrice, termometara, pa čak i svetala ili zvučnika. Najjednostavniji način da se obezbedi ažurnost svih uređaja je da se, kad god je to moguće, omogući automatsko ažuriranje.
4. **Antivirus**: Svi grešimo, te ponekad kliknemo ili instaliramo nešto što ne bi trebalo i što može da zarazi naše sisteme malverom. Antivirus je tu da nas zaštiti od takvih grešaka. Iako antivirus ne može da zaustavi sav malver, on pomaže da se otkriju i zaustave česti dobro poznati napadi. Zbog toga obezbedite da svi kućni računari imaju instaliran antivirusni softver, kao i da on bude ažuran i aktivan. Pored navedenog, mnoga današnja antivirusna rešenja uključuju i druge bezbednosne tehnologije poput fajervola i zaštite veb-pregledača (browser).
5. **Rezervne kopije**: Kada ništa drugo ne pomaže, rezervne kopije su često jedini način za oporavak od grešaka poput brisanja podataka ili od sajber napada kao što je Ransomware. Postarajte se da vaši rođaci i prijatelji koriste automatizovan sistem za izradu bekapa. Najjednostavnija rešenja za izradu bekapa su često bazirana na Cloud tehnologijama i obezbeđuju da se bekap kreira svakog sata ili kad god se neki fajl promeni. Ova rešenja pojednostavljuju ne samo izradu bekapa, već i oporavak podataka iz bekapa.

Deljenjem ovih pet jednostavnih saveta pomozite drugima da na bezbedan način maksimalno iskoriste tehnologije.

Zaštita dece u gostima

Ako ste "na ti" sa tehnologijom, verovatno ste se već postarali da i vi i vaša deca budete bezbedni prilikom njenog korišćenja. Međutim, kada vaše dete boravi u poseti prijateljima ili rođacima, poput bake i deke, oni možda ne znaju kako da zaštite decu na Internetu niti kakva su vaša očekivanja. U nastavku su koraci koji vam mogu pomoći da zaštitite decu dok borave u poseti kod drugih:

- **Pravila**: Obezbedite da, ako postoje pravila ili očekivanja koje imate u pogledu bezbednosti dece, drugi obavezno znaju za njih. Na primer, postoje li pravila po pitanju vremena koje dete može provesti na Internetu, sa kim može

Pomozite drugima da budu bezbedni

da komunicira ili koje igre može/ne može da igra? Nije dobro da prepustite detetu da ono samo upozna druge sa ovim pravilima. Dobro rešenje je da napravite spisak pravila koji ćete dostaviti svima koje vaše dete često posećuje.

- **Kontrola**: Ako dete razume tehnologiju bolje od osoba koje se o njemu staraju, moguće je da će tu prednost pokušati da iskoristi. Na primer, deca mogu da traže ili otkriju kredencijale za nalog sa administratorskim pravima na dedinom računaru i potom urade šta god žele, na primer instaliraju igricu koju ne želite da igraju. Potrudite se da rođaci razumeju da deci ne treba da daju dodatna prava mimo onoga što je dogovoreno.

Na kraju, predložite bliskim ljudima da se prijave da dobijaju informacije poput OUCH! biltena koji će im pomoći da nastave da se sami edukuju. Ovaj bilten se objavljuje jednom mesečno na preko 20 jezika. Prijava je dostupna na https://securingthehuman.sans.org/ouch.

Saznajte više

Prijavite se na OUCH! mesečni bilten za podizanje svesti o bezbednosti informacija namenjen svima, pročitajte prethodne brojeve OUCH!-a i saznajte više o SANS-ovim rešenjima za unapređenje svesti o bezbednosti informacija na našoj internet prezentaciji securingthehuman.sans.org/ouch/archives.

Verzija na srpskom

Telekom Srbija kao društveno odgovorna telekomunikaciona kompanija pomaže prevođenje i distribuciju ovog biltena kako bi se unapredila svest korisnika informaciono-komunikacionih tehnologija o bezbednosti informacija.

Dodatne informacije

Socijalni inžinjering:	https://securingthehuman.sans.org/ouch/2017#january2017
Pristupne fraze:	https://securingthehuman.sans.org/ouch/2017#april2017
Menadžeri lozinki:	https://securingthehuman.sans.org/ouch/2017#september2017
Verifikacija iz dva koraka:	https://securingthehuman.sans.org/ouch/2015#september2015
Rezervne kopije i oporavak:	https://securingthehuman.sans.org/ouch/2017#august2017
Zaštita dece na Internetu:	https://securingthehuman.sans.org/ouch/2017#may2017

Redakcija: Walt Scrivens, Phil Hoffman, Кэти Клик, Cheryl Conley
Preveli: Dragan Ristić i Gordana Živanović