Mesečni bilten bezbednosnih saveta za korisnike računara

OUCH!

U OVOM IZDANJU...

- Uvod
- Zašto si meta
- Kako da se zaštitiš

Da, i ti si takođe meta

Uvod

Uobičajena zabluda običnih ljudi je da oni nisu meta sajber kriminalaca, da oni ili njihov računar nemaju takav značaj i vrednost. Takvo ubeđenje je veoma pogrešno. Ako poseduješ računar, mobilni uređaj, on-line račun, adresu el. pošte, kreditnu karticu ili si uključen u bilo kakvu on-line aktivnost, onda si svakako interesantan sajber kriminalcima. U ovom izdanju objasnićemo zašto si i ti meta, kako mogu da te napadnu, i šta možeš da preduzmeš da bi se zaštitio.

Gost urednik

Eric Conrad je presednik i CTO Backshore Communications-a i glavni autor knjiga „CISSP Study Guide, Second Edition“ i „Eleventh Hour CISSP, Second Edition“. Takođe je koautor šestodnevnog kursa „Continuous Monitoring and Security Operations“ (SEC511) pri SANS-u.

Zašto si meta

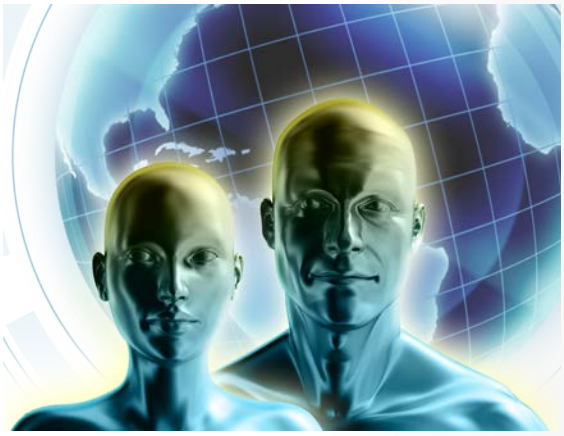
Zločini kao što su prevara, krađa identiteta ili iznuda postoje od kada postoji civilizacija, oni su deo našeg svakodnevnog života. Cilj kriminalaca je uvek isti: da naprave što više novca, što lakše je moguće, i sa što manje rizika. Tradicionalno, je to bilo teško zato što su kriminalci bili uslovljeni lokacijom i potrebom da imaju fizičku interakciju sa potencijalnom žrtvom. Na takav način, kriminalci ne samo da su bili ograničeni koga mogu da napadnu, nego je i rizik kome se izlažu bio veoma visok. Međutim, sa pojavom Interneta i on-line tehnologija kriminal se radikalno promenio. Danas, sajber kriminalci mogu jednostavno da naciljaju skoro svakog na svetu, sa malo ili bez ikakvih troškova, i uz veoma mali rizik. Osim toga, sajber kriminalci su postali veoma organizovani i efikasni, što im omogućava da budu uspešniji nego ikada.

Konačno, sajber kriminalci su svesni da što više kreditnih kartica ili lozinki ukradu, to više novca mogu da zarade. Samim ti će pokušati da hakuju svakog ko je konektovan na Internet, uključujući i tebe. Hakovanje miliom ljudi širom sveta se čini kao ogroman posao, ali je ustvari veoma lako obzirom da se

© The SANS Institute 2014

Da, i ti si takođe meta

koriste automatizovani alati. Na primer, moguće je kreirati bazu sa milionima adresa el. pošte i upotrebiti automatske alate da na te adrese pošalju el. poruke za sajber pecanje. Slanje takvih poruka skoro da ništa ne košta, jer se obično u tu svrhu koriste unapred hakovani računari, moguće čak i tvoj. To je jedan primera da i tvoj računar ima neku vrednost, može da se koristiti za hakovanje drugih računara. Na kraju, kriminalci unapred ne znaju ko će se sve „upecati“ na njihove el. poruke, ali znaju da što više el. poruka pošalju veća je verovatnoća da se neko „upeca“. Moguće je da u pretrazi za računarima koje mogu da hakuju, kriminalci pokušaju da skeniraju sve računare na Internetu (moguće i korišćenjem tvog računara). Imaj na umu da sajber kriminalci napadaju svakoga , uključujući i tebe, i da ni u čemu nisi drugačiji od miliona osoba koje su već bile hakovane ili prevarene.



Možda toga nisi svestan, ali tvoji uređaji i informacije imaju ogromnu vrednost za sajber kriminalce širom sveta.

Kako da se zaštitiš

Kada sajber kriminalci pokušaju da hakuju milione ljudi širom sveta koriste prilično jednostavne metode. Na sreću, primenom jednako jednostavnih koraka, moguće je da se zaštitiš:

- Ti: Prva linija odbrane od sajber napada si ti. Mnogi sajber napadi se zasnivaju na pokušaju napadača da te prevari da otvoriš inficiranu el. poštu ili da otkriješ svoju lozinku preko telefona. Zdrav razum je najbolja odbrana, ako je nešto čudno, sumljivo ili previše dobro da bi bilo istinito, najverovatnije je da se radi o prevari.
- Ažuriranje: Budi siguran da je računar ili mobilni uređaj koji koristiš ažuriran i da su instalirane najnovije zakrpe. To važi ne samo za operativni sistem nego i za aplikacije ili dodatke koje koristiš. Redovno ažuriranje sistema i aplikacija pomaže u zaštiti od najčešćih i najrasprostranjenih napada.

© The SANS Institute 2014

Da, i ti si takođe meta

- Lozinke: Koristi jaku, jedinstvenu lozinku za svaki svoj račun. Na taj način ako je vebsajt koji koristiš hakovan i kompromitovane su sve lozinke, ostali tvoji računi su sigurni. Takođe budi siguran da su svi tvoji uređaji zaštićeni lozinkom, PIN-om ili nekim drugim mehanizmom za zaključavanje. Da bi pamtio sve soje lozinke preporučljivo je korišćenje Menadžera Lozinki.
- Kreditne kartice: Redovno proveravaj stanje na svojim bankovnim računima, preporučljivo je bar nedeljno. Ako primetiš ne autorizovanu transakciju po nekoj kartici, odmah je prijavi kompaniji koja je karticu izdala. Ako tvoja banka omogućava uslugu slanja obaveštenja putem el. pošte ili poruke prilikom većih transakcija, obavezno je koristi.
- Tvoja mreža: Obezbedi svoju kućnu WI-FI mrežu jakom administratorskom lozinkom i osiguraj da zahteva lozinku priliko povezivanja svakog uređaja. Budi siguran da znaš koji su uređaji povezani na tvoju mrežu i da su svi ažurirani.
- Društvene Mreže: Što više informacija objavljuješ po društvenim mrežama, to je veći rizik po tvoju on-line bezbednost. Ne samo da informacije koje objavljuješ mogu da olakšaju kriminalcima da te lakše prevare, nego te mogu okarakterisati kao metu vrednu njihovog truda.

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

OUCH! Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Securing Your Home Network:	http://www.securingthehuman.org/ouch/2014#january2014
OUCH! Phishing Attacks:	http://www.securingthehuman.org/ouch/2013#february2013
Poster: You Are A Target:	http://www.securingthehuman.org/resources/posters

OUCH! Objavljuje SANS Securing The Human program i distribuira se pod Creative Commons BY-NC-ND 3.0 licencom.
Biltene je dozvoljeno distribuirati ili koristiti za svoj program unapređenja bezbednosne svesti uz uslov da sadržaj nije modifikovan.
U vezi prevoda ili za dodatne informacije, kontaktiraj ouch@securingthehuman.org.

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