Mesečni bilten bezbednosnih saveta za korisnike računara

OUCH!

U OVOM IZDANJU...

Društvene mreže

Uvod

Društvene mreže, kao što su Facebook, Twitter, Instagram i LinkedIn, predstavljaju neverovatne resurse, koji nam omogućavaju da se upoznajemo, komuniciramo i razmenjujemo informacije sa ljudima širom sveta. Međutim, sve te neverovatne mogućnosti sa sobom nose određeni rizik, ne samo za vas, nego i za vašu porodicu, prijatelje i poslodavca. U ovom izdanju objasnićemo opasnosti koje vrebaju i kako da društvene mreže koristite bezbedno i sigurno.

Gost urednik

Tanya Baccam je dugogodišnji konsultant za bezbednost. Preko deset godina je autor i instruktor SANS kurseva, uključujući SEC502, SEC542, SEC401, MGT414, AUD507. Možete je pratiti na Tweeter-u na **@tbaccam**.

Privatnost

Opšte je mišljenje da je glavni problem prilikom korišćenja društvenih mreža zaštita ličnih informacija. Potencijalne opasnosti takođe uključuju:

- **Uticaj na vašu budućnost**: Neki poslodavci prilikom zapošljavanja proveravaju profile kandidata na društvenim mrežama. Neprikladne ili inkriminišuće fotografije ili objave, bez obzira kada su objavljene, mogu da budu razlog da ne dobijete posao ili unapređenje. Takođe, mnogi univerziteti primenjuju istu praksu prilikom prijema novih studenata. Opcije privatnosti vam neće biti od velike koristi ako vam takve organizacije zatraže da „Lajkujete“ ili pristupite njihovoj stranici, a takođe imajte na umu da sve što objavljujete može da se prenese i arhivira na nekim drugim Internet stranicama.
- **Napadi na vas**: Sajber kriminalci mogu da analizom onoga što objavljujete dođu do pravih zaključaka i da ih iskoriste da pristupe vašim ili informacijama vaše organizacije. Na primer, informacije koje delite sa drugima mogu da iskoriste da pogode odgovor na vaše „tajno pitanje“ za resetovanje lozinke, kreiranje ciljane el. pošte za napad „pecanjem“, ili da pozovu nekog iz vaše organizacije pretvarajući se da ste vi. Osim toga, rizici se mogu preneti u fizički sve, pošto se lako može identifikovati gde radite ili živite.
- **Nenamerno nanošenje štete svom poslodavcu**: Kriminalci ili konkurenti mogu da, sve osetljive informacije o vašem poslodavcu koje objavljujete, iskoriste protiv vašeg poslodavca. Osim toga, imajte na umu da informacije koje objavljujete mogu da nanesu štetu reputaciji vašeg poslodavca. Budite sigurni da ste pre nego objavite nešto o svom poslu ili poslodavcu, proverili bezbednosne politike vaše organizacije, a takođe imajte na umu da ono što objavljujete po društvenim mrežama, u nekim slučajevima, može da bude nadgledano.

Društvene mreže

Najbolju zaštitu predstavlja limitiranje informacija koje objavljujete. Tačno je da opcije privatnosti mogu da obezbede određenu zaštitu, ali su često zbunjujuće i veoma se često menjaju bez vašeg znanja. Nešto što ste mislili da je privatno veoma brzo može da postane javno iz mnogo razloga. Osim toga, privatnost informacija koje objavljujete je bezbedna koliko su to ljudi sa kojima ih delite. Sa što više prijatelja i kontakta podelite neku informaciju, to je veća verovatnoća da postane javna. Uvek treba da imate na umu da bilo šta što objavite može ili će postati javno i zauvek objavljeno na Internetu.

Konačno, budite upoznati sa onim što vaši prijatelji objavljuju o vama. Ako objave nešto sa čime niste saglasni ili je neprijatno za vas, zatražite im da to obrišu. Ako odbiju, kontaktirane društvenu mrežu na kojoj je objavljeno i zatražite od njih da obrišu sadržaj u vezi vas. Samim tim imajte obzira šta i kakve informacije objavljujete o drugim osobama.



Društvene mreže su zabavne i moćne, ali uvek vodite računa koje informacije objavljujete i ko može da im pristupi.

Bezbednost

Osim saveta vezanih za privatnost informacija, preporučujemo vam nekoliko saveta koji mogu da dodatno doprinesu bezbednosti vaših naloga i aktivnosti na društvenim mrežama:

- **Prijavljivanje (login)**: Obezbedite sve vaše naloge sa jakom, jedinstvenom lozinkom i nemojte je deliti sa drugima. Osim toga, mnoge društvene mreže podržavaju jače (pouzdanije) metode autentifikacije, kao što je verifikacija iz dva koraka. Uvek kada je to moguće, koristite takve metode autentifikacije. Konačno, nemojte koristi vaš nalog za društvenu mrežu za prijavljivanje na druge Internet servise, zato što u tom slučaju ako je jedan od naloga hakovan, svi ostali su ugroženi.
- **Podešavanja privatnosti**: Ako koristite opciju podešavanja privatnosti, budite sigurni de je redovno proveravate i testirate. Društvene mreže često menjaju politiku privatnosti i samo podešavanje, pa je lako napraviti grešku. Pored toga, mnoge aplikacije i servisi dozvoljavaju da svojoj objavi pridodate svoju lokaciju (geotagging). Ako želite da ne objavljujete svoju lokaciju redovno proveravajte ova podešavanja.
- **Enkripcija**: Društvene mreže uglavnom koriste HTTPS ekripciju u cilju obezbeđenja vaše veze sa njihovom Internet stranicom. Neke od njih, kao Twitter i Google+ to omogućavaju kao podrazumevano podešavanje, dok je kod drugih potrebno da sami podesite, omogućite HTTPS. Proveriti kakav je trenutni status HTTPS na društvenim mrežama koje koristite i ako postoji takva opcija a još nije u funkciji, uključite je.
- **El. pošta**: Budite oprezni sa el. poštom koja izgleda kao da dolazi sa društvenih mreža, pošto često može da se radi o lažnoj el. pošti koja se koristi za sajber napade. Najsigurniji način da se odgovori na ovakvu poštu je da se

Društvene mreže

prijavite direktno na samu društvenu mrežu, bez upotrebe linkova iz same el. pošte, i da onda pročitate i odgovorite na sve eventualne poruke i obaveštenja.

- **Štetni linkovi/prevare**: Budite oprezni sa linkovima ili potencijalnim prevarama objavljenim na društvenim mrežama. Sajber kriminalci često koriste društvene mreže sa svoje napade. Iako nekad izgleda da je poruku objavio neko od vaši prijatelja, to često ne mora da bude tačno, pošto njihovi nalozi takođe mogu da budu hakovani. Ako je neki od vaših članova porodice ili prijatelja objavio čudnu i neočekivanu poruku koju ne možeš da proveriš (na primer da je opljačkan i da je potrebno da mu pošalješ novac), pozovite ga telefonom i kontaktirajte ga na neki drugi način da bi proverili da li objavljena poruka tačna.
- **Mobilne aplikacije**: Većina društvenih mreža ima i svoje verzije mobilnih aplikacija, u cilju lakšeg korišćenje sa mobilnih uređaja. Takve aplikacije uvek preuzimajte iz proverenih izvora i zaštitite svoj mobilni uređaj sa jakom lozinkom. Ako vaš pametni telefon nije zaključan kada ga izgubite, svako ko ga fizički poseduje može da pristupi vašim nalozima na društvenim mrežama, i da objavljuje informacije u vaše ime.

Društvene mreže su izuzetan medijum za komunikaciju i druženje sa ljudima širom sveta. Ako se pridržavate saveta koje smo naveli u ovom izdanju, moći ćete da uživate u bezbednijem korišćenju i iskustvu. Ako želite da naučite više o bezbednom korišćenju društvenih mreža koje koristite ili da prijavite neovlašćeno korišćenje, proverite na samim Internet stranicama društvenih mreža.

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

Dodatne informacije

Propusne fraze:	http://www.securingthehuman.org/ouch/2015#april2015
Verifikacija iz dva koraka:	http://www.securingthehuman.org/ouch/2013#august2013
Bezbedno korišćenje mobilnih aplikacija:	http://www.securingthehuman.org/ouch/2015#january2015
Edukacija dece u vezi sajber bezbednosti:	http://www.securingthehuman.org/ouch/2015#june2015
Bezbednost na Facebook-u:	https://www.facebook.com/safety

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