OUCH! | 2015.gada jūlijs

Ikmēneša biļetens par informācijas tehnoloģiju drošību datoru lietotājiem

OUCH!

ŠAJĀ NUMMURĀ …

Sociālie tīkli

Ievads

Sociālo mediju vietnes kā Facebook, Twitter, Instagram un LinkedIn ir apbrīnojami resursi, kas dod iespēju Jums tikties, sadarboties un dalīties ar cilvēkiem visā pasaulē. Tomēr ar iespējām kopā nāk riski ne tikai Jums, bet arī Jūsu ģimenei, draugiem un darba devējam. Šajā izdevumā aprakstīsim šos apdraudējumus, kā arī dosim padomus, kā pareizi un droši izmantot šīs vietnes.

Viesredaktors

Tanya Baccam ir drošības konsultante ar ilggadēju pieredzi. Viņa ir bijusi SANS autore un pasniedzēja vairāk kā desmit gadus, ieskaitot SEC502, SEC542, SEC401, MGT414, AUD507 un daudzus citus kursus. Sekojiet viņai Twitter **@tbaccam**.

Privātums

Izmantojot sociālos medijus, jārūpējas par savas personīgās informācijas aizsardzību. Iespējamie apdraudējumi ir:

- Ietekme uz Jūsu nākotni: Organizācijas mēdz izmantot sociālo mediju vietnes informācijas ievākšanai par potenciālo darbinieku. Neatkarīgi no tā, cik sen veikts inkriminējošs ieraksts vai publicēts apkaunojošs foto, tas var nākotnē neļaut Jums saņemt paaugstinājumu amatā vai Jūs var nepieņemt darbā. Arī daudzas universitātes mēdz veikt līdzīgas pārbaudes studentu pieteikumiem. Privātuma uzstādījumi ne vienmēr var Jūs pasargāt, jo šīs organizācijas var Jūs aicināt nospiest “Like” vai pievienoties viņu vietnēm, kā arī noteikti ieraksti var būt arhivēti vairākās vietās.
- Pret Jums vērsti uzbrukumi: Uzbrucēji var analizēt Jūsu ierakstus un izmantot tos, lai piekļūtu Jūsu vai Jūsu organizācijas informācijai. Piemēram, tie var izmantot informāciju, ko Jūs publicējat, lai uzminētu atbildes uz “slepenajiem” jautājumiem un nomainītu Jūsu paroles, izveidotu tieši pret Jums vērstus mērķētus uzbrukumus, ko dēvē par “spearfishing”, vai piezvanītu kādam Jūsu organizācijā, izliekoties par Jums. Uzbrukumi var pārcelties arī fiziskajā pasaulē, piemēram, nosakot, kur Jūs dzīvojat vai strādājat.
- Nejauši nodarīt ļaunumu Jūsu darba devējam: Noziedznieki vai konkurenti var izmantot pret Jūsu darba devēju jebkuru sensitīvu informāciju, ko Jūs publicējat par savu darbavietu. Jūsu ieraksti var potenciāli kaitēt organizācijas reputācijai. Uzziniet, kāda ir organizācijas politika, pirms publicējat kaut ko par savu darbu, īpaši ņemot vērā, ka Jūsu ierakstus sociālo mediju vietnēs organizācija var uzraudzīt.

Sociālie tīkli

Labākā aizsardzība ir ierobežot savu ierakstu saturu. Jā, privātuma iestatījumi var nodrošināt zināmu aizsardzību, tomēr tie mēdz būt neskaidri formulēti un var bieži mainīties, jums to pat nezinot. Tas, ko Jūs uzskatījāt par privātu, var ātri vien kļūt publisks dažādu iemeslu dēļ. Jūsu ierakstu privātums ir tikai tik drošs, cik droši ir cilvēki, ar kuriem Jūs dalāties. Jo ar vairāk draugiem vai kontaktiem Jūs vēlaties dalīties, jo ticamāk ir tas, ka šī informācija kļūs publiska. Drošāk ir uzskatīt, ka jebkas, ko Jūs publicējat, kļūst publisks un kļūst par Interneta neatņemamu un mūžīgu sastāvdaļu.

Visbeidzot, sekojiet līdzi tam, ko draugi un kontakti raksta par Jums. Ja viņi publicē kaut ko, kas Jums šķiet nepieņemams, lūdziet viņiem to izdzēst. Ja viņi atsakās vai ignorē Jūs, sazinieties ar sociālo mediju vietni un lūdziet viņiem izdzēst attiecīgo ierakstu. Tāpat ar cieņu izturieties pret to, ko Jūs publicējat par citiem.



Sociālo mediju vietnes ir interesantas un iespaidīgas, taču esiet uzmanīgi ar to, ko Jūs publicējat un kam tas ir pieejams.

Drošība

Bez privātuma apdraudējumiem šeit ir daži ieteikumi, kā aizsargāt Jūsu sociālo mediju kontus un tiešsaistes aktivitātes.

- Pieteikšanās: savi konti jāaizsargā ar stipru, unikālu paroli, ko nevajag atklāt nevienam. Daudzas sociālo mediju vietnes piedāvā stiprāku autentifikācijas aizsardzību, piemēram, divu faktoru verifikāciju. Ja iespējams, izmantojiet šo papildu aizsardzību. Neizmantojiet savu sociālo mediju kontu, lai pierakstītos citās vietnēs, jo, ja tās tiek uzlauztas, tad apdraudēti ir arī Jūsu konti.
- Privātuma iestatījumi: Ja Jūs izmantojat privātuma iestatījumus, regulāri tos pārskatiet un pārbaudiet. Bieži sociālo mediju vietnes izmaina privātuma iestatījumus un ir ļoti viegli kļūdīties, izvēloties nepareizos iestatījumus. Daudzas aplikācijas un servisi dod iespēju pievienot raksturlielumus saturam, ko Jūs publicējat (piemēram, geotagging (atrašanās vietas pazīme)). Regulāri pārbaudiet iestatījumus, ja vēlaties, lai Jūsu atrašanās vieta ir privāta.
- Šifrēšana: Sociālo mediju vietnes izmanto šifrēšanu (HTTPS), lai pasargātu Jūsu pieslēgumu vietnei. Dažas vietnes, tādas kā Twitter un Google+, to nodrošina pēc noklusējuma, citām nepieciešams šo iestatījumu ieslēgt. Pārbaudiet savus konta iestatījumus un ieslēdziet HTTPS kā noklusējuma savienojumu, kur vien iespējams.
- E-pasts: Izturieties ar aizdomām pret e-pastiem, kas apgalvo, ka nāk no sociālo mediju vietnēm, jo tie var būt ļaundaru sūtīti uzbrukuma mēģinājumi. Drošākais veids, kā rīkoties ar ziņojumiem, ir pierakstīties tieši sociālo mediju vietnē un tad izlasīt un atbildēt uz vietnes ziņojumiem.
- Ļaundabīgas saites/Krāpniecība: Esiet piesardzīgi ar aizdomīgām saitēm vai sociālo mediju vietnēs publicētiem

Sociālie tīkli

iespējamiem krāpniecības mēģinājumiem. Ļaundari izmanto sociālos medijus savu uzbrukumu izplatīšanai. Tikai tādēļ, ka ieraksts nācis no drauga konta, nenozīmē, ka paziņojums tiešām nāk no viņa, drauga konts var būt kompromitēts. Ja draugs vai ģimenes loceklis ir publiskojis dīvainu ierakstu, (piemēram, ka tie ir apzagti un lūdz Jūs nosūtīt viņiem naudu), mēģiniet piezvanīt viņiem, lai pārliecinātos, vai ziņa ir patiesa.

- Mobilās aplikācijas: Vairums sociālo mediju vietņu piedāvā mobilās aplikācijas, lai Jūs varētu piekļūt saviem tiešsaistes kontiem. Pārliecinieties, ka vietne, no kuras lejupielādējat šīs aplikācijas, ir uzticama. Noteikti aizsargājiet savu mobilo telefonu ar stipru paroli. Ja telefons ir atbloķēts, kad jūs to pazaudējat, jebkurš, kas piekļūst Jūsu tālrunim, var izmantot sociālo mediju vietnes, izliekoties par Jums.

Sociālo mediju vietnes ir brīnišķīgs veids, kā sazināties un uzturēt sakarus ar pasauli. Ievērojot augstāk minētos ieteikumus, Jūs varat padarīt savas tiešsaistes aktivitātes ievērojami drošākas. Lai uzzinātu vairāk par to, kā droši izmantot šīs vietnes, vai ziņotu par neautorizētu aktivitāti, apmeklējiet attiecīgās sociālo mediju vietnes drošības lapu.

UZZINIET VAIRĀK

Parakstieties uz OUCH! - ikmēneša biļetenu par informācijas tehnoloģiju drošību datoru lietotājiem, apmeklējiet OUCH! arhīvu, uzziniet vairāk par SANS informācijas tehnoloģiju drošības risinājumiem, apmeklējot tīmekļa vietni http://www.securingthehuman.org.

CERT.LV ir Latvijas Republikas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā. Uzziniet vairāk https://www.cert.lv vai sekojiet mums Twiterī @certlv.

Resursi

Paroļu frāzes:	http://www.securingthehuman.org/ouch/2015#april2015
Divu faktoru verifikācija:	http://www.securingthehuman.org/ouch/2013#august2013
Mobilo aplikāciju droša lietošana:	http://www.securingthehuman.org/ouch/2015#january2015
Bērnu izglītošana par kiberdrošību:	http://www.securingthehuman.org/ouch/2015#june2015
Facebook drošība:	https://www.facebook.com/safety

License

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Tulkojums: Edgars Tauriņš