

OUCH!

Ikmēneša informācijas drošības izdevums tev

Sociālo mediju privātums

Pārskats

Lielākajai daļai cilvēku pat prātā neienāktu doma ieliet cilvēku pilnā telpā un pilnīgiem svešiniekiem skaļi paziņot dažādus savas privātās dzīves aspektus, sākot no veselības problēmām, līdz ģimenes locekļu un draugu vārdiem, vecumiem, darba vietām vai skolu atrašanās vietām. Bet bieži vien šie paši cilvēki pat neminstināsies pirms publicēt šādu informāciju sociālajos tīklos. Neapdomīgi izpausta informācija var radīt negatīvu ietekmi ne tikai uz jūsu personīgo un profesionālo dzīvi, bet arī ietekmēt jūsu ģimeni un draugus.

Sociālie tīkli ir lieliska vieta, kur atjaunot kontaktus, dalīties un mācīties. Taču pārliecināšanās, ka jūsu privātuma iestatījumi ir gana droši, nav vienīgais veids, kā varat sevi pasargāt. Tiklīdz jūs kaut ko publicējat tiešsaistē, jūs pazaudējat pār to kontroli. Jums jāsaprot, kāda informācija tiek ievākta un kā tā tiek izmantota. Šeit būs pāris privātuma aspekti, par kuriem būtu jāpadomā, izmantojot sociālos medijus:



Privātuma iestatījumi: Uzmanīgi izvēlieties un regulāri pārskatiet visu jūsu sociālo mediju kontu privātuma iestatījumus, jo īpaši ja tiek veiktas izmaiņas pakalpojuma izmantošanas nosacījumos un privātuma nosacījumos. Atcerieties, ka pat tad, ja esat atļāvis piekļuvi jūsu veidotajam saturam tikai ierobežotam cilvēku lokam, visa jūsu informācija tiek apkopota, izanalizēta un uzglabāta sociālo mediju serveros, iespējams, mūžīgi.



Privātuma Koks: Sociālo mediju iestatījumi nevar jūs pasargāt no jūsu draugiem, radniekiem un kolēģiem, kuriem ir tiesības aplūkot jūsu ziņas, un tiesības ar tām dalīties savu draugu lokā u.c.



Informācija par ģimeni: Visiem patīk runāt par viņu draugiem un ģimeni. Bet publicējot muļķīgas dzimšanas dienu bildes, vai veselības un uzvedības problēmas var novest pie vardarbības izturēšanās, īpaši jaunākā vecuma bērniem, un var atstāt ietekmi uz visu atlikušo mūžu.



Informācijas publicēšana: Ja pakalpojums ir bez maksas, tad jūs esat produkts. Izpētes rezultātā ir noskaidrots, ka tas, ko jūs darāt tiešsaistē, var tikt pārdots kādam citam.



Vietas informācija: Piereģistrēšanās informācija var tikt pievienota pārējiem jūsu personas datiem, lai izveidotu profilu par jūsu dzīvi un ieradumiem, kas var novest pie izsekošanas un pakļaut jūs citu uzņēmīgu aktivitāšu riskam. Ņemiet vērā arī to, ka attēliem vai video, kurus publicējat, iespējams, ir pievienota lokācijas informācija.



Mākslīgais intelekts: Mākslīgais intelekts, sociālie mediji un mārketingi ir perfekta kombinācija. Mūsdienā mārketingi izmanto informāciju par jūsu uzvedību un paradumiem tiešsaistē, lai piegādātu jums reklāmu, kas saistīta ar pēdējiem meklētajiem atslēgvārdiem vai pēdējo pirkumu, tādējādi turpinot iegūt arvien vairāk informācijas par jums.



Digitālā nāve: Kad kāda persona nomirst, tās tiešsaistes resursi tiek pakļauti īpašam ļaunprātīgu uzbrukumu riskam, ja vien kontus neturpina uzturēt vai neaizver palicēji. Individuālais privātums vairs neattiecas tikai uz viņu vienu pašu; tas var ietekmēt arī viņa ģimenes locekļus un draugus.



Netīša informācijas izpaušana: Informācija, kuru par sevi publicējat, var daudz pavēstīt par jūsu personīgo vēsturi, tādējādi atklājot atbildes uz jūsu tiešsaistes drošības jautājumiem.

Privātums ir kas daudz vairāk par privātuma iestatījumiem jūsu sociālā tīkla kontā. Jo vairāk jūs dalāties ar informāciju par sevi un jo vairāk informācijas par jums publicē citi, jo vairāk informācijas ievāc un izmanto korporācijas, valdības un citi. Viens no labākajiem veidiem, kā sevi pasargāt, ir rūpīgi pārdomāt un samazināt tās informācijas apjomu, ko par sevi publicējat un ko citi publicē par jums, neatkarīgi no tā, kāds privātuma līmenis šai informācijai tiek uzstādīts.

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 Twitterī [@certlv](https://twitter.com/certlv).

Viesredaktors

Cathy Click ir vairāk nekā 14 gadus ilga pieredze drošības izglītības programmu veidošanā globālā mēroga Fortune 500 kompānijai. Cathy patīk izvēlēties sarežģītas tehniskas tēmas un "iztulkot" tās viegli saprotamā valodā, lai palīdzētu cilvēkiem uzlabot savu tiešsaistes drošību.



Resursi

Digitālais mantojums: <http://www.sans.org/u/Z2G>

Krāpšana sociālajos tīklos: <http://www.sans.org/u/Z2L>

Vai tev ir rezerves kopijas?: <http://www.sans.org/u/Z2Q>

OUCH! izdod SANS institūts programmas "Security Awareness" ietvaros un tas tiek izplatīts saskaņā ar [Creative Commons BY-NC-ND 4.0 licences nosacījumiem](https://creativecommons.org/licenses/by-nc-nd/4.0/). Jūs varat izplatīt šo biļetenu vai izmantot to savā informācijas tehnoloģiju drošības izglītības programmā ar nosacījumu, ka biļetens netiek izmainīts. Papildu informācijai vai jautājumiem par tulkošanu izmantojiet www.sans.org/security-awareness/ouch-newsletter e-pasta adresi. Redakcija: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Tulkojums: CERT.LV