

OUCH!

Ikmēneša informācijas drošības biļetens ikvienam

Ieteikumi sociālo tīklu drošai lietošanai

Ievads

Sociālie tīkli, piemēram, Snapchat, Facebook, Twitter, Instagram un LinkedIn ir lieliski resursi, kas ļauj jums tikties un komunicēt ar cilvēkiem visā pasaulē. Tomēr šīs iespējas slēpj arī riskus. Riskus ne tikai jums, bet arī jūsu ģimenei, draugiem un darba devējam. Šajā izdevumā piedāvājam ieteikumus, kā pēc iespējas drošāk lietot sociālos tīklus.

Publicēšana

Pirms informācijas publicēšanas visu kārtīgi apdomājiet. Viss, ko jūs publicēsiet, visticamāk kādā brīdī kļūs publiski pieejams, un var negatīvi iespaidot jūsu reputāciju un nākotni, ieskaitot to, kurā skolā jūs iesiet vai kādu darbu iegūsiet. Ja nevēlaties, lai jūsu ģimene vai darba devējs kaut ko redzētu, labāk to vienkārši npublicēt sociālajos tīklos. Esiet piesardzīgi – arī citi par jums var kaut ko publicēt. Iespējams, jums pat vajadzēs pieprasīt, lai kāds dzēš informāciju, ko par jums ir publicējis.

Privātums

praktiski visos sociālajos tīklos ir pieejamas papildu privātuma iespējas, - uzstādiet tās, kad vien tas ir iespējams. Piemēram, vai mājaslapai tiešām nepieciešams zināt jūsu atrašanās vietu? Papildu privātuma iespējas var būt sarežģītas un tās bieži mainās. Izveidojiet ieradumu regulāri tās pārbaudīt un pārlicināties, vai tās strādā tā, kā jūs esat iedomājies.

Paroles

aizsargājiet savu sociālo tīklu kontus ar pietiekami garu, unikālu paroli vai paroles frāzi. Paroles frāze ir parole, kas sastāv no vairākiem vārdiem, padarot to viegli iegaumējamu un uzrakstāmu, bet daudz grūtāk uzminamu kiber noziedzniekiem.

Aizsargājiet savu kontu

vēl labāk, uzstādiet divu faktoru autentifikāciju visiem jūsu kontiem. Tas pievieno papildu autentifikācijas faktoru (parasti gadījuma skaitli, kas katru reizi mainās) parolei, kad jūs vēlaties ieiet savā kontā. Šobrīd tas ir vienkārši, un tā ir viena no labākajām aizsardzības metodēm.

Krāpniecība

līdzīgi kā ar e-pastiem, arī sociālo tīklu paziņojumus var izmantot dažādiem krāpniecības mēģinājumiem. Piemēram, ļaundaris var mēģināt izvilināt jūsu paroli vai kredītkartes informāciju. Esiet piesardzīgiattiecībā uz saitēm, ko saņemat: draugs, kurš atsūta jums dīvainu ziņu vai kaut ko, kas nav viņam raksturīgs, visticamāk var izrādīties ļaundaris, kas tikai izliekas par jūsu draugu.

Lietošanas noteikumi

iepaizīstieties ar sociālo tīklu lietošanas noteikumiem – jebkas, ko jūs publicējat, var kļūt par sociālo tīklu īpašumu.

Darbs

ja vēlaties publicēt kaut ko par savu darbu, vispirms noskaidrojiet, vai tas ir pieņemami jūsu vadībai.

Aicinām ievērot sniegtos ieteikumus, lai padarītu savu tiešsaistes pieredzi daudz drošāku un patīkamāku. Lai uzzinātu vairāk par to, kā droši izmantot sociālos tīklus vai ziņot par nepieļaujamām aktivitātēm, izpētiet attiecīgā sociālā tīkla drošības sadaļu.

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

Jessica Barker ir viena no vadošajām speciālistēm pasaulē cilvēka kiberdrošības jomā. Viņa ir [Redacted Firm](#) līdzdibinātāja. Šajā uzņēmumā viņa sniedz konsultācijas klientiem visā pasaulē, un bieži uzstājas arī dažādās konferencēs. Jessica Barker twitter konts: [@drjessicabarker](https://twitter.com/drjessicabarker).



Resursi

Paroļu frāzes: <https://www.sans.org/u/B6E>
Divu soļu verifikācija: <https://www.sans.org/u/B6J>
Bērnu drošība tiešsaistē: <https://www.sans.org/u/B6O>
Padariet savu kontu drošāku: <https://www.lockdownyourlogin.org/>

License

OUCH! izdod SANS institūts programmas “Securing The Human” ietvaros un tas tiek izplatīts saskaņā ar [Creative Commons BY-NC-ND 4.0 licences nosacījumiem](#). 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, Cathy Click, Cheryl Conley | Tulkojums: Edgars Tauriņš