OUCH! 2021. gada

Privātums – jūsu digitālā nospieduma aizsardzība

Kas ir privātums?

Pastāv dažādas privātuma definīcijas. Koncentrēsimies uz personīgo privātumu, aizsargājot informāciju, ko citi ievāc par jums. Jūs pārsteigtu, cik daudz un dažādas organizācijas mūsdienu digitālajā pasaulē ne tikai ievāc informāciju par jums, bet pēc tam šo informāciju arī legāli izplata vai pārdod. Ikreiz, kad tiešsaistē kaut ko pārlūkojat vai iegādājaties, skatāties videoklipu, pērkat pārtiku, apmeklējat ārstu vai izmantojat kādu lietotni savā viedtālrunī, viedtelevizorā vai citā mājas ierīcē, par jums tiek ievākta informācija. Šo informāciju var izmantot, lai jums pārdotu preces vai pakalpojumus, noteiktu procentu likmi jūsu aizdevumam, izlemtu par jums pieejamo ārstniecību vai darba vietām. Turklāt, ja šī informācija nonāk nepareizajās rokās, kibernoziedznieki to var izmantot, lai padarītu jūs par mērķi un uzbruktu jums.

Personīgā privātuma pārvaldīšanas mērķis ir kontrolēt jūsu digitālo nospiedumu, t.i. - mēģināt aizsargāt un ierobežot informāciju, kas par jums tiek apkopota. Jums ir jāsaprot, ka mūsdienu digitālajā pasaulē ir gandrīz neiespējami neradīt digitālo nospiedumu vai neļaut nevienai organizācijai ievākt informāciju par jums – varam to tikai ierobežot.

Soļi, ko varat spert, lai palīdzētu aizsargāt jūsu privātumu

Nav viena soļa, ar kuru varētu novērst visus ar privātumu saistītos riskus. Tā vietā jums būs jāsper dažādi soļi, un katrs no tiem kaut nedaudz palīdzēs sargāt privātumu. Jo vairāk soļu spersiet, jo vairāk palīdzēsiet aizsargāt jūsu privātumu.

- Ierobežojiet saturu, kuru ievietojat un kuram ļaujat piekļūt, piemēram, publiskos forumos vai sociālajos tīklos. Tāpat jābūt piesardzīgiem ar attēliem vai pašbildēm, ar kurām dalāties. Pat tad, ja publicējat ierakstus privātos forumos vai izmantojot spēcīgus privātuma iestatījumus, jāpieņem, ka jebkurš jūsu ieraksts kādā brīdī kļūs publiski pieejams.
- Veidojot tiešsaistes kontus, pārskatiet Privātuma politikas sadaļu, lai uzzinātu kādu informāciju vietnes par jums ievāc, un sniedziet tikai nepieciešamāko informāciju. Ja jums rada bažas vietnes ievāktā informācija, neizmantojiet šo vietni.
- Jums ir jāsaprot, ka neatkarīgi no jūsu izvēlētajiem privātuma iestatījumiem, par jums tiek ievākta informācija, jo īpaši tādās bezmaksas vietnēs kā Facebook un WhatsApp. Šie pakalpojumi balsta savu biznesa modeli uz datu ievākšanu par to, ko darāt, un ar ko kontaktējaties. Ja jums patiesi rūp jūsu privātums, neizmantojiet šādas bezmaksas vietnes.

- Izpētiet mobilā tālruņa lietotnes pirms lejupielādējiet un uzstādiet tās. Vai to izstrādātājs ir uzticams? Vai tās bijušas pieejamas jau ilgu laiku? Vai tām ir daudz pozitīvu atsauksmju? Pārbaudiet pieprasītās piekļuves tiesības. Vai mobilā tālruņa lietotnei tiešām jāzina jūsu atrašanās vieta un vajadzīga piekļuve jūsu kontaktiem? Ja nejūtaties pārliecināti, izvēlieties citu lietotni. Meklējiet lietotnes, kas atbalsta privātumu un piedāvā jums izvēles iespējas. Kaut arī par lietotni, kas ievēro jūsu privātumu, var nākties maksāt vairāk, tas var izrādīties tā vērts.
- Apsveriet virtuālā privātā tīkla (VPN) lietošanu saviem interneta pieslēgumiem, īpaši tad, ja izmantojat publisko tīklu, piemēram, bezmaksas WiFi.
- Izmantojot interneta pārlūku, uzstādiet privātuma iestatījumus uz "privāts" vai "inkognito", lai ierobežotu par jums pieejamo informāciju, to, kā tiek izmantotas un uzglabātas jūsu sīkdatnes, un aizsargātu jūsu pārlūkošanas vēsturi. Apsveriet privātuma paplašinājumu lietošanu, piemēram, Privacy Badger vai uz privātumu orientētu pārlūkprogrammu.
- Apsveriet anonīmu meklētājprogrammu izmantošanu, kas veidotas ar mērķi nodrošināt privātumu, piemēram, DuckDuckGo vai StartPage.

Privātuma aizsardzība daudzējādā ziņā ir ļoti sarežģīta, jo tas lielā mērā atkarīgs no likumdošanas un privātuma prasībām, kādas noteikusi valsts, kurā dzīvojat, un to uzņēmumu ētika, ar kuriem jums ir darīšana. Lai gan šajā tehnoloģiju laikmetā nekādi nevarat pilnībā aizsargāt savu privātumu, šie soļi palīdzēs jums ierobežot par jums apkopotās informācijas daudzumu.

Viesredaktors

Kenton Smith ir ievērojams kiberdrošības konsultants un padomdevējs Kalgari, Kanādā, kurš specializējas drošības programmu izstrādē, pārvaldībā un izvērtēšanā. Viņš pasniedz nodarbības SANS menedžmenta programmā, un viņu varat atrast Twitter kā @kentonsmith vai reizēm sastapt kentonsmith.net.

Resursi

Privātuma iestatījumu uzstādīšana: https://staysafeonline.org/stay-safe-online/managing-your-privacy/manage-privacy-settings/
Aizsardzība pret identitātes zādzību: https://www.sans.org/security-awareness-training/resources/identity-theft
Virtuāls privātais tīkls: https://www.sans.org/security-awareness-training/resources/virtual-private-networks-vpns
Publiski pieejamas informācijas pārbaude: https://www.sans.org/security-awareness-training/resources/search-yourself-online

Tulkojums: CERT.LV