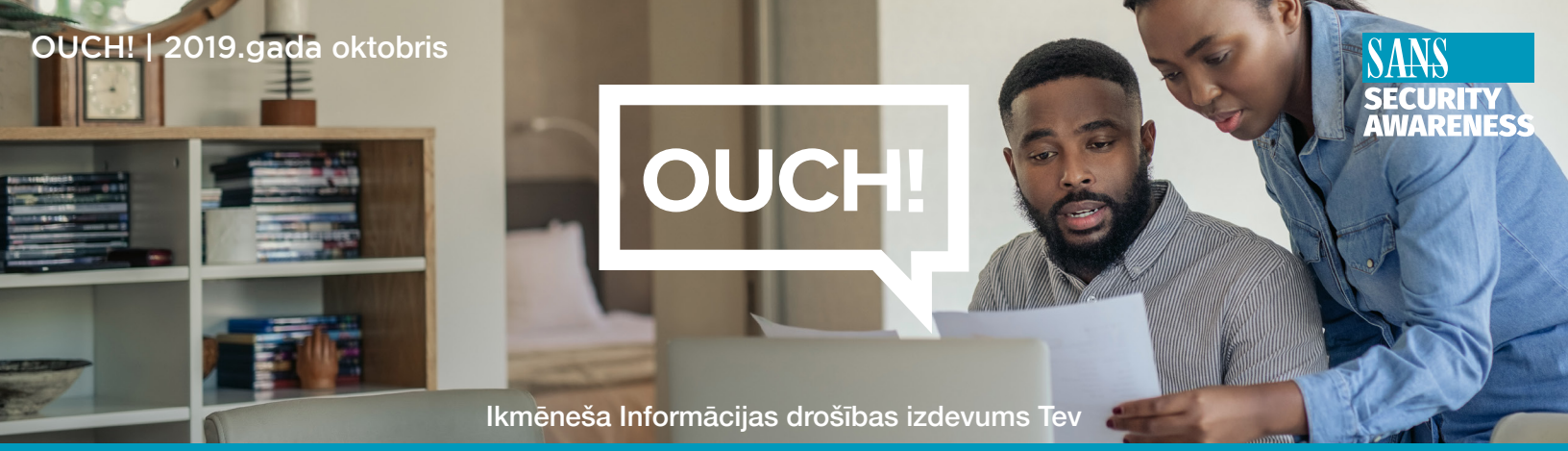

Ikmēneša Informācijas drošības izdevums Tev

Četri soļi, lai saglabātu drošību

Pārskats

Tehnoloģijas mūsdienās mums sniedz neierobežotas un neidomājamas iespējas, tāpēc nereti var šķist mulsinoši un pat nomācoši, visu laiku domāt līdzi, kā tās izmantot droši. Taču, neatkarīgi no tā, kādas tehnoloģijas jūs izmantojat, vai kā jūs tās izmantojat, zemāk apkopota informācija par četriem vienkāršiem soļiem drošākai tehnoloģiju izmantošanai:

1. Jūs: Pirmkārt un galvenokārt, tehnoloģijas vienas pašas nespēs jūs pasargāt! Jūs paši esat jūsu labākais sargs. Uzbrucēji ir iemācījušies, ka labākais vieds, kā iegūt to, ko viņi vēlas, ir uzbrūkot jums, nevis jūsu datoram vai citām iekārtām. Ja viņiem interesē jūsu parole, jūsu maksājumu kartes dati, vai kontrole pār jūsu datoru, viņi centīsies ar viltu panākt, ka jūs to viņiem iedodat, visbiežāk saziņā ar jums radot steidzamības sajūtu. Piemēram, viņi var jums piezvanīt un izlikties par Microsoft tehniskā atbalsta dienesta pārstāvi un apgalvot, ka jūsu dators ir inficēts, kaut patiesībā viņi ir kibernoziedznieki, kas grib iegūt piekļuvi jūsu datoram. Jeb varbūt viņi nosūtīs jums e-pastu, kurā paziņos, ka nav iespējams nosūtīt jūsu pasta sūtījumu, un mēģinās jūs piārliecināt atvērt e-pastā norādīto saiti, lai apstiprinātu jūsu sūtījuma adresi, kaut patiesībā viņi centīsies ievilināt jūs krāpnieciskā vietnē, kas centīsies uzlauzt jūsu datoru. Tāpēc labākā aizsardzība pret uzbrukumu esat jūs paši. Domājiet kritiski, vērtējiet informāciju, jo tikai jūs paši tā varat pamanīt, atpazīt un apturēt virkni uzbrukumu.

2. Paroļu frāzes: Moderno datoru darbības un skaitļošanas ātrumi ir padarījuši tradicionālo 8-simbolu paroli novecojušu un ievainojamu. Kad vietne lūdz jums izveidot paroli, 8-simbolu paroles vietā veidojiet drošu, unikālu paroļu frāzi. Paroļu frāze ir tāda parole, kurā tiek izmantota virkne vārdu, kurus ir jums viegli atcerēties, kā piemēram, "bite medus lietus ledus". Jo garāka ir paroļu frāze, jo tā ir drošāka. Neaizmirstiet, ka nepieciešams atšķirīgiem kontiem un iekārtām izmantot atšķirīgas un unikālas paroļu frāzes. Ja viena paroļu frāze tiek kompromitēta, jūsu pārējie konti un iekārtas joprojām ir drošībā. Nevarat atcerēties visas izveidotās paroļu frāzes? Izmantojiet paroļu pārvaldnieku (password manager) – tā ir specializēta programma vai lietotne, kas visas izveidotās paroļu frāzes uzglabā drošā, šifrētā veidā, ir pieejamas gan maksas gan bezmaksas programmas/lietotnes, un parasti šīm ir arī daudz citu lielisku funkciju.

Visbeidzot, aktivitzējiet divu faktoru verifikāciju/autentifikāciju Šī pieeja izmanto gan jūsu paroli, gan pievieno papildu soli, piemēram, kodu, kas tiek nosūtīts uz jūsu viedtālruni, vai lietotni, kas ģenerē papildus drošības kodu. Divu faktoru verifikācija , iespējams, ir vissvarīgākais solis, ko varat spert, lai pasargātu savus tiešsaistes kontus, un tās lietošana ir daudz vienkāršāka nekā jums varētu likties.

3. Regulāri atjauniniet programmatūru: Pārliecinieties, ka katrā iekārtā, kuru izmantojat regulāri, tiek lejupielādēti un uzstādīti atjauninājumi. Kiberuzbrucēji nepārtraukti meklē programmatūru ievainojamības, un, tās atklājot, rada īpašas programmas, kas ļauj ievainojamības izmantot, lai piekļūtu jūsu iekārtām un tajās esošajai informācijai. Programmatūru ražojošās organizācijas, savukārt, regulāri publicē atjauninājumus, kuru uzstādīšana var pasargāt pret atklātajām ievainojamībām. Nodrošinot, ka jūsu datorā, mobilajā tālrunī vai citā viedierīcē atjauninājumi tiek regulāri uzstādīti, jūs sevi pasargājat labāk. Vislabāk un ērtāk ir aktivizēt automātisko atjauninājumu uzstādīšanu, tā nodrošinot ka nepalaidīsiet nevienu svarīgu atjauninājumu garām. Atcerieties, ka atjauninājumi uzstādāmi ikvienai ierīcei, kas ir pieslēgta internetam – TV, novērošanas kameras, mājas interneta rūteri, spēļu konsoles un pat jūsu automašīna.

4. Veidojiet rezerves kopijas: Neskatoties uz to, cik uzmanīgi esam, mēs ikviens varam tik pakļauti kiberuzbrukumu riskam – mūsu datori, telefoni un citas viedierīces var tikt uzlauztas un ļaundari var piekļūt mums svarīgai informācijai. Ja tā notiek, tad vienīgais veids sevis pasargāšanai un informācijas saglabāšanai ir rezerves kopiju veidošana. Pārliecinieties, ka regulāri veidojat rezerves kopijas un pārliecinieties, ka vienmēr varat atkal piekļūt jums svarīgajai informācijai no šīm rezerves datu glabāšanas vietām. Lielākā daļa operētājsistēmu un mobilo iekārtu mūsdienās piedāvā automātisku rezerves kopiju veidošanu, sinhronizējot informāciju vai nu ārējos datu nesējos vai mākoņdatošanas pakalpojumos. (cloud computing services).

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.

Viesredaktors

*Stīvs Ansons (**Steve Anson**) ir SANS sertificēts lektors. Viņš sniedz padomus IT drošības ekspertu komandām un valstu valdībām visā pasaulē. Stīvs ir topošās grāmatas "Praktiskā incidentu risināšana" autors, un vietnē www.AppliedIncidentResponse.com regulāri publicē bezmaksas materiālus IT drošības speciālistiem.*

Resursi

Sociālā inženierija:	https://www.sans.org/u/W3G
Personalizēta krāpšana:	https://www.sans.org/u/W3Q
Kā padarīt paroles vieglāk iegaumējamas:	https://www.sans.org/u/W3V
Vai tev ir rezerves kopijas?:	https://www.sans.org/u/W40

Redakcija: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Tulkojums: CERT.LV