Ikmēneša informācijas drošības izdevums tev

Paroļu pārvaldnieki

Pārskats

Viens no svarīgākajiem veidiem, kā varat sevi pasargāt, ir lietot katram kontam un lietotnei unikālu un sarežģītu paroli. Diemžēl, ir gandrīz neiespējami atcerēties visas atšķirīgās paroles. Turklāt, mēs arī zinām, cik laikietilpīgi ir katru reizi dažādās vietnēs ievadīt savas paroles, ģenerēt jaunas, censties izsekot atbildēm uz visiem drošības jautājumiem, kā arī daudzi citi faktori. Taču tam ir risinājums, kas atvieglos jūsu ikdienu un vienlaikus padarīs to drošāku - paroļu pārvaldnieks.

Kā strādā paroļu pārvaldnieks

Paroļu pārvaldnieks glabā visas jūsu paroles vienotā datu bāzē, kuru mēz saukt arī par paroļu maciņu. Paroļu pārvaldnieks sašifrē jūsu paroļu maciņa saturu un aizsargā to ar tā saukto ģenerālo paroli (master password), kuru zināt tikai jūs. Brīdī, kad jums vajadzīga kāda parole, lai autentificētos e-pasta vietnē vai interneta bankā, jūs vienkārši ievadāt ģenerālo paroli un atverat savu paroļu maciņu. Paroļu pārvaldnieks automātiski piemeklēs atbilstošo paroli un drošā veidā atvērs pieeju pieprasītajai vietnei. Līdz ar to jums turpmāk vairs nebūs jāatceras visas paroles un jāvada tās manuāli, lai piekļūtu kādai vietnei.

Turklāt, lielākajai daļai paroļu pārvaldnieku ir iespēja automātiski sinhronizēt paroles starp visām piekļuves iekārtām. Šādā situācijā, ja atjaunosiet paroli kādai vietnei, piemēram klēpjdatorā, tad šīs izmaiņas tiks sinhronizētas un būs aktīvas arī citās ierīcēs. Visbeidzot, lielākā daļa paroļu pārvaldnieku redz, kad jūs veidojat jaunu tiešsaistes kontu vai atjaunināt esošā konta paroli, un tie automātiski atjaunina informāciju jūsu paroļu maciņā.

Tāpēc ir ļoti svarīgi, lai ģenerālā parole, ar kuru jūs aizsargājat paroļu pārvaldnieku, būtu pietiekoši gara un unikāla. Mēs rekomendējam ģenerālo paroli veidot kā frāzi vai izteicienu, izmantojot vairākus vārdus. Ja jūsu paroļu pārvaldnieks atbalsta divu soļu autentifikāciju, tad savai ģenerālparolei noteikti lietojiet arī to. Kopumā jums jāatceras un jālieto tikai ģenerālā parole. Ja jūs to aizmirsīsiet, jūs nevarēsiet tikt klāt citām parolēm.

Kā izvēlēties paroļu pārvaldnieku

Ir tik daudz paroļu pārvaldnieku, kā izvēlēties piemērotāko? Resursu sadaļā ir saite, kurā jūs varat iepazīties ar vairāku paroļu pārvaldnieku pārskatiem. Kamēr izvēlaties sev piemērotāko, paturiet prātā:

Jūsu paroļu pārvaldnieka lietošanai ir jābūt vienkāršai. Ja piedāvātais risinājums ir pārāk sarežģīts, jāatrod cits, kas jums der labāk.

Paroļu pārvaldniekam ir jāstrādā uz visām iekārtām, kurās jums jāvada paroles. Būtu jābūt vienkārši sinhronizēt visas paroles visās jūsu iekārtās.

Izmantojiet tikai labi pazīstamus un uzticamus paroļu pārvaldniekus. Esiet piesardzīgi attiecībā uz rīkiem, kas ir pieejami tikai nesen, vai par kuriem nav nemaz vai ir ļoti neliels skaits atsauksmju. Kibernoziedznieki var piedāvāt viltus paroļu pārvaldniekus, lai nozagtu jūsu informāciju. Esiet piesardzīgi arī gadījumos, kad ražotājs apgalvo, ka izmanto paša izstrādātu šifrēšanas mehānismu.

Izvairieties no paroļu pārvaldniekiem, kuri apgalvo, ka spēj atjaunot jūsu ģenerālo paroli. Tas nozīmē, ka viņi zina jūsu ģenerālo paroli, kas, savukārt, pakļauj jūs pārlieku lielam riskam.

Lai arī kuru risinājumu jūs izvēlētos, pārliecinieties, ka ražotājs aktīvi nodrošina atjauninājumus un drošības ielāpus un ka vienmēr lietojat jaunāko produkta versiju.

Paroļu pārvaldniekam būtu jāpiedāvā iespēja saglabāt arī citu jums svarīgu un sensitīvu informāciju, kā, piemēram, atbildes uz drošības jautājumiem, kredītkartes datus, klienta karšu informāciju.

Apsveriet iespēju ievietot savu ģenerālo paroli aizzīmogotā aploksnē slēgtā skapī, seifā vai slēdzamā kastē.

Paroļu pārvaldnieks ir lielisks veids, kā droši glabāt visas savas paroles un citu sensitīvo informāciju, kā piemēram, kredītkartes datus. Taču pārliecinieties, ka lietojat unikālu un stipru ģenerālo paroli, kā arī vienmēr izmantojat jaunāko risinājuma versiju, lai kurš arī tas būtu.

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

Russell Eubanks *ir daudzkārtēji sertificēts informācijas drošības eksperts no Atlantas ar vairāk kā 20 gadu pieredzi. Viņš ir viens no SANS Internet Storm Center incidentu risinātājiem kā arī ir piedalījies SANS "The CIS Critical Security Controls" tapšanā. Russell ir sasniedzams @russelleubanks un https://www.securityeverafter.com.*

Resursi

Kā padarīt paroles vieglāk iegaumējamas:	http://www.sans.org/u/10Uu
Digitālais mantojums:	http://www.sans.org/u/10Uz
Wired labāko paroļu pārvaldnieku apskats (ENG):	https://www.wired.com/story/best-password-managers/

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