

Ikmēneša informācijas drošības biļetens ikvienam

OUCH!

ŠAJĀ NUMMURĀ ...

- Pārskats
- Kā darbojas paroļu pārvaldnieki
- Paroļu pārvaldnieka izvēle

Paroļu pārvaldnieki

Pārskats

Lai sevi pasargātu, viens no svarīgākajiem aspektiem ir drošas un unikālas paroles izmantošana katram savam kontam un aplikācijai. Diemžēl ir praktiski neiespējami atcerēties dažādās paroles dažādiem kontiem. Tādēļ tik daudz cilvēku izmanto vienas un tās pašas paroles atkārtoti. Diemžēl tas ir bīstami, jo, ja kāds uzmin vai iegūst jūsu paroli, viņš var piekļūt visiem kontiem, kur šī parole izmantota. Vienkāršs risinājums ir izmantot paroļu pārvaldnieku vai paroļu seifu. Tā ir programma, kas uzglabā visas jūsu paroles, tādējādi dodot iespēju izmantot unikālas un drošas paroles katram kontam. Izmantojot paroļu pārvaldnieku ir jāatceras tikai viena parole – galvenā parole pašam paroļu pārvaldniekam.

Viesredaktors

Chris Christianson ir informācijas drošības konsultants Kalifornijā ar 20 gadu pieredzi un vairākiem tehniskajiem sertifikātiem. Viņš ir uzstājies dažādās konferencēs un ir daudzu industrijas rakstu autors. Viņu var sasniegt [@cchristianson](https://twitter.com/cchristianson) un <https://ismellpackets.com>.

Kā strādā paroļu pārvaldnieki

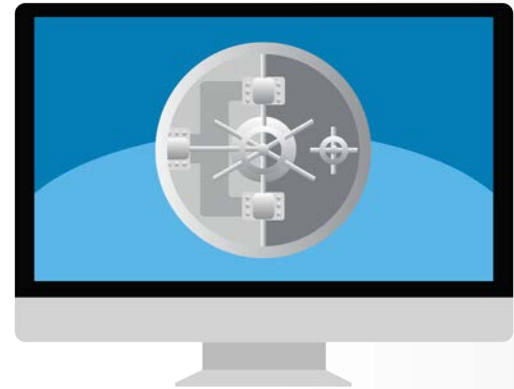
Paroļu pārvaldnieki saglabā visas jūsu paroles datu bāzē, ko dēvē arī par paroļu seifu. Paroļu pārvaldnieks nošifrē bāzes saturu un aizsargā to ar galveno paroli, kas zināma tikai jums. Kad nepieciešams ievadīt paroles, piemēram, pieslēgties interneta bankai vai e-pastam, jūs ievadat galveno paroli pārvaldniekā, lai atslēgtu informāciju bāzē. Vairumā gadījumu paroļu pārvaldnieks var arī automātiski ievadīt paroli un pieslēgties jūsu vietā. Tas ļauj jums izmantot simtiem unikālu drošu paroļu, jo jums tās nav jāatceras.

Daži paroļu pārvaldnieki glabā informāciju jūsu datorā vai mobilajā ierīcē, kamēr citi saglabā to mākonī. Papildus vairums piedāvā iespēju automātiski sinhronizēt paroļu bāzi visās ierīcēs, kurās jūs atļaujat iespēju piekļūt pārvaldniekam. Tādējādi, kad jūs aktualizējat vai izveidojat paroli datorā, izmaiņas tiek sinhronizētas arī citās ierīcēs (planšetē, mobilajā telefonā). Neatkarīgi no tā, kur tiek uzglabāta datu bāze, jums nepieciešams instalēt pārvaldnieka programmu, lai jūsu sistēma vai iekārta varētu to izmantot.

Paroļu pārvaldnieki

Uzsākot izmantot paroļu pārvaldnieku, jums manuāli jāievada vai jāimportē jūsu lietotājvārdi un paroles. Pēc tam paroļu pārvaldnieks var noteikt, vai veicat jaunu reģistrāciju tiešsaistes kontā vai esošās paroles maiņu, un izdarīt atbilstošas izmaiņas datu bāzē. Tas tādēļ, ka vairums paroļu pārvaldnieku sadarbojas ar tīmekļa pārlūku. Šāda integrācija ļauj arī automātiski pieslēgties mājas lapās.

Ļoti būtiska ir galvenās paroles drošība – tai jābūt pietiekami sarežģītai un tādai, kuru nav iespējams uzminēt. Mēs iesakam izmantot šīm vajadzībām paroļu frāzi. Ja paroļu pārvaldnieks dod iespēju izmantot divu faktoru verifikāciju, izmantojiet šo iespēju. Visbeidzot, vienmēr atcerieties savu galveno paroli, jo, ja jūs to pazaudēsiet vai aizmirsīsiet, jūs zaudēsiet iespēju piekļūt citām parolēm.



Paroļu pārvaldnieki ir vienkāršs veids kā uzglabāt un lietot visas jūsu daudzās paroles.

Paroļu pārvaldnieka izvēle

Iespējams ir izvēlēties no daudziem pārvaldniekiem. Resursu sadaļā ir atrodama saite uz paroļu pārvaldnieku apskatiem. Lai atrastu sev piemērotāko, vēlams atcerēties sekojošo:

- Paroļu pārvaldniekam jābūt vienkāršam lietošanā. Ja risinājums ir pārāk sarežģīts vai nesaprotams, labāk atrodiet tādu, kas ir saprotams un piemērots tieši jums.
- Paroļu pārvaldniekam jāspēj strādāt uz visām jūsu ierīcēm, kurās jūs izmantojat paroles. Sinhronizācijai arī jābūt pietiekami vienkāršai un saprotamai.
- Izmantojiet labi zināmus un uzticamus paroļu pārvaldniekus. Uzmantieties no produktiem, kas ir salīdzinoši jauni vai kam nav sabiedrības atsauksmes. Noziedznieki var izveidot viltotus paroļu pārvaldniekus jūsu informācijas nozagšanai. Esiet aizdomīgi arī pret ražotājiem vai izplatītājiem, kas izmanto paši savu šifrēšanas risinājumu.
- Neizmantojiet pārvaldnieku, kas piedāvā atgūt jūsu galveno paroli. Tas nozīmē, ka viņiem tā ir pieejama, kas ir pārāk riskanti, jo tad jūsu parolēm var piekļūt kāds cits.

Paroļu pārvaldnieki

- Pārliecinieties, ka ražotājs regulāri atjaunina risinājumu, un vienmēr izmantojiet jaunāko versiju.
- Paroļu pārvaldniekā ir jābūt iespējai automātiski ģenerēt drošas paroles un parādīt jums paroļu drošības līmeni.
- Paroļu pārvaldniekam jāpiedāvā iespēja saglabāt arī citus datus, piemēram, atbildes uz drošības jautājumiem vai citu personīgo informāciju.

Paroļu pārvaldnieki ir labs līdzeklis jūsu paroļu un citu sensitīvo datu uzglabāšanai. Tā kā tie uzglabā ļoti svarīgu informāciju, vienmēr izmantojiet unikālu un drošu galveno paroli, kuru ir ne tikai sarežģīti uzminēt kādam citam, bet arī vienkārši atcerēties jums.

UZZINIET VAIRĀK

Parakstieties uz OUCH! - ikmēneša biļetenu par informācijas tehnoloģiju drošību datoru lietotājiem, apmeklējiet OUCH! arhīvu, uzziniet vairāk par SANS informācijas tehnoloģiju drošības risinājumiem, apmeklējot tīmekļa vietni securingthehuman.sans.org/ouch/archives.

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).

Resursi

- Paroļu pārvaldnieku 2017.gada tops: <https://www.pcmag.com/article2/0,2817,2407168,00.asp>
- Paroļu frāzes: <https://securingthehuman.sans.org/ouch/2017#april2017>
- Divu pākāpju verifikācija: <https://www.securingthehuman.org/ouch/2015#september2015>
- Jūsu pieslēgšanās aizsardzība: <https://www.lockdownyourlogin.org/>
- SANS dienas drošības ieteikums: <https://www.sans.org/tip-of-the-day>

License

OUCH! izdod SANS institūts programmas "Securing The Human" ietvaros un tas tiek izplatīts saskaņā ar [Creative Commons BY-NC-ND 3.0 licences](https://creativecommons.org/licenses/by-nc-nd/3.0/) nosacījumiem. Jūs varat izplatīt šo biļetenu vai izmantot to savā informācijas tehnoloģiju drošības izglītošanas programmā ar nosacījumu, ka biļetens netiek izmainīts Papildu informācijai vai jautājumiem par tulkošanu izmantojiet www.securingthehuman.org/ouch e-pasta adresi.

Redakcija: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley

Tulkotājs: Edgars Tauriņš

