Ikmēneša informācijas drošības biļetens ikvienam

OUCH!

ŠAJĀ NUMMURĀ …

Paroļu frāzes

Ievads

Paroles ir kaut kas, ko mēs izmantojam praktiski katru dienu, sākot no pieejas e-pastam vai internetbankai līdz viedtālruņa izmantošanai un interneta veikaliem. Tomēr paroles var būt arī jūsu vājā vieta. Ja kāds uzzina vai uzmin jūsu paroli, tad viņš var piekļūt jūsu kontiem tāpat kā to varētu jūs, tādā veidā pārskaitot jūsu naudu, lasot jūsu e-pastus vai nozogot jūsu identitāti. Tādēļ drošas paroles ir būtiskas jūsu aizsardzībai. Tomēr paroles parasti ir grūti atcerēties un sarežģīti ievadīt. Šajā izdevumā jūs uzzināsiet, kā izveidot drošas paroles, ko viegli atcerēties un vienkārši ievadīt – tās tiek sauktas par paroļu frāzēm.

Viesredaktors

My-Ngoc Nguyen ir sertificēta SANS instruktore un Secured IT Solutions vadītāja/vadošā konsultante. Viņa ir ieguvusi vairākus sertifikātus un viņai ir vairāk kā 14 gadu pieredze kiberdrošības programmu izstrādei dažādām industrijām un sektoriem. Twitter: **@MenopN** LinkedIn: My-Ngoc “Menop” Nguyen.

Paroļu frāzes

Izaicinājums mums visiem ir tas, ka kibernoziedznieki ir izstrādājuši izsmalcinātas un efektīvas metodes paroļu automātiskai minēšanai (brute force). Tas nozīmē, ka ļaundari var uzzināt jūsu paroles, ja tās ir vājas vai viegli uzminamas. Svarīgs solis sevis aizsardzībai ir drošu paroļu izmantošana. Parasti tas tiek darīts, izmantojot sarežģītas paroles, tomēr tās ir grūti atcerēties, tās ir mulsinošas un tās ir grūti ievadīt. Tādēļ iesakām izmantot paroļu frāzes – dažādus nesaistītus vārdus vai teikumu. Jo garāka ir jūsu paroļu frāze, jo tā ir drošāka. Frāzes ir vienkāršāk atcerēties un ierakstīt, taču joprojām sarežģīti uzminēt. Divi dažādi piemēri:

Uzglabāt-Viegli-Ieslodzīt
Tējas laiks 13:23

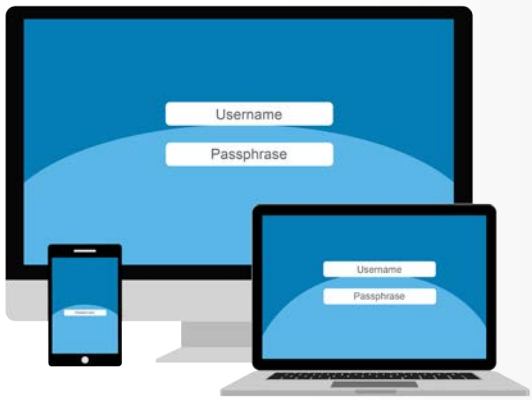
Frāzes drošas padara ne tikai tas, ka tās ir garas, bet arī ka tās izmanto lielos burtus un simbolus (atcerieties, arī atstarpes un interpunkcijas zīmes ir simboli). Tajā pašā laikā paroļu frāzes ir viegli atcerēties un uzrakstīt. Jūs varat padarīt frāzi vēl drošāku, aizstājot burtus ar cipariem vai simboliem, piemēram, “a” ar “@” simbolu vai “o” burtu ar ciparu “0”. Ja mājas

Paroļu frāzes

lapa vai programma ierobežo paroles garumu, izmantojiet maksimālo iespējamo simbolu skaitu.

Paroļu frāžu droša izmantošana

Protams, arī izmantojot paroļu frāzes, ir jāievēro piesardzība. Frāžu izmantošana nepalīdzēs, ja ļaundari var tās viegli nozagt vai nokopēt.



Paroļu frāzes ir vienkāršāks veids kā izveidot un atcerēties drošas paroles.

1. Katram kontam vai ierīcei izmantojiet citu frāzi. Piemēram, nekad neizmantojiet vienu un to pašu paroli jūsu darba vai bankas kontiem un personīgajiem kontiem Facebook, YouTube vai Twitter. Tādā veidā, ja kāds no šiem kontiem tiek uzlauzts, citi konti ir drošībā. Ja jums ir pārāk daudz paroļu frāzes, lai tās atcerētos (kas bieži notiek), izmantojiet paroļu pārvaldnieku. Tā ir programma, kas droši uzglabā jūsu paroļu frāzes. Šādā gadījumā jums ir jāatceras tikai paroles, kas nepieciešamas jūsu iekārtai un paroļu pārvaldniekam.
2. Neatklājiet nevienam savu paroļu frāzi vai principu, kā jūs to izveidojat, nevienam, ieskaitot kolēģus un vadītāju. Atcerieties, paroles frāze ir noslēpums; ja kāds cits to zina, paroles frāze vairs nav droša. Gadījumā, ja jūs nejauši atklājat frāzi kādam, vai jums ir aizdomas, ka tā varētu būt nozagta, nekavējoties to nomainiet. Vienīgais izņēmums, ja jūs vēlaties uzticēt jūsu personīgās paroles frāzes uzticamam cilvēkam ārkārtas gadījumiem. Iespējams ir arī uzrakstīt savas paroles frāzes, noglabāt tās drošā vietā un pateikt par šo drošo vietu uzticamam cilvēkam, piemēram, tuvam ģimenes loceklim. Tādā veidā, ja kaut kas atgadās ar jums un ir nepieciešama palīdzība, kādam ir iespēja piekļūt jūsu kontiem.
3. Neizmantojiet publiskos datorus, piemēram, viesnīcās vai interneta kafejnīcās, piekļuvei jūsu kontiem. Ņemot vērā to, ka šādus datorus var izmantot jebkurš, tie var būt inficēti un tie var uzkrāt informāciju par jūsu taustiņu nospiedieniem. Piekļūstiet jūsu kontiem tikai no uzticamiem datoriem vai mobilām ierīcēm.
4. Esiet piesardzīgi, kad tīmekļa vietne prasa jums atbildes uz personīgas dabas jautājumiem. Šādus jautājumus var izmantot gadījumos, ja jūs aizmirstat savu paroles frāzi un to nepieciešams atjaunot. Problēma ir tā, ka atbildes uz šiem jautājumiem var atrast internetā vai pat jūsu Facebook lapā. Šādos gadījumos dodiet tikai tādas atbildes, kuras nav publiski pieejamas vai arī izdomājiet atbildes. Gadījumā, ja nevarat atcerēties, kādas atbildes ierakstījāt, varat

Paroļu frāzes

veidot atbildes, balstoties uz noteiktu tēmu, piemēram, filmas vai grāmatas varoni. Otra iespēja ir atkal izmantot paroļu pārvaldnieku, kur iespējams saglabāt arī papildu informāciju.

5. Daudzi tiešsaistes konti piedāvā t.s. divu faktoru autentifikāciju, kas ir zināma arī kā divu soļu verifikācija. Šādā gadījumā jums nepieciešms vēl kaut kas papildus bez paroļu frāzes, lai piekļūtu kontam, piemēram, kods, ko nosūta uz jūsu telefonu. Šāda metode ir daudz drošāka, kā tikai paroles izmantošana. Kad vien iespējams, izmantojiet šādas drošākas autentifikācijas metodes.
6. Mobilās ierīces parasti prasa PIN kodu, lai piekļūtu. Atcerieties – PIN nav nekas vairāk kā cita parole. Jo jūsu PIN ir garāks, jo tas ir drošāks. Daudzas mobilās ierīces ļauj jums mainīt savu PIN kodu, izmantot paroļu frāzi vai izmantot biometriju, piemēram, pirksta nospiedumu.
7. Ja jūs vairāk neizmantojat kontu, dzēsiet, slēdziet vai atspējojiet to.

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 Twiterī @certlv.

Resursi

Paroļu pārvaldnieks: https://securingthehuman.sans.org/ouch/2015#october2015

Divu soļu verifikācija: https://securingthehuman.sans.org/ouch/2015#september2015

Kontrolē savu pieslēgšanos: https://lockdownyourlogin.com

SANS SEC301 – Piecu dienu kurss kiberdrošības pamatos: https://sans.org/sec301

License

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

Tulkojums: Edgars Tauriņš