Co-funded by the
Erasmus+ Programme
of the European Union

Drošu paroļu izveidošana

Saturs

Drošu paroļu izveides un pārvaldības vadlīnijas

Katru datora vai vietnes (vai cita resursa) lietotāju atpazīst pēc lietotāja pieteikšanās vārda un paroles. Šos datus glabā kā noslēpumu, un tos nedrīkst atklāt pat kolēģiem vai radiniekiem.

Bieži vien vienu datoru lieto vairāki cilvēki. Pat mājās katram lietotājam ir individuāls pieteikšanās vārds un parole. Tad katra lietotāja vide, iestatījumi, dokumentu glabāšanas vietas tiks nodalītas un aizsargātas no citiem datora lietotājiem.

Ja lietotājiem ir noteiktas tiesības, kopīgos datoros ir pietiekami iestatīt vairākus dažādus lietotāju tipus, piemēram, darba vietā. Piemēram, pārvaldnieks varētu izmantot lielāko daļu organizācijas resursu, piekļūt datu bāzēm, savukārt citiem lietotājiem varētu būt ierobežotas pieejas tiesības datiem. Vēl viens lietotājs varētu būt administrators, kuram ir visas tiesības un kurš var pielāgot visus datora un informācijas sistēmu iestatījumus.

Ikdienas lietošanai priekšroka tiek dota ierobežotam kontam, jo visa šī lietotāja pārvaldītā programmatūra, ieskaitot vīrusus, bez viņa ziņas iegūst šī lietotāja tiesības. Jo mazāk lietotājam ir tiesības, jo mazāk kaitējumu var nodarīt ļaunprātīga programmatūra.

Kādēļ ir svarīgi izveidot spēcīgas paroles?

Hakeriem ir vairākas metodes:

- **visbiežāk lietoto paroļu izmēģināšana:** hakeri var viegli atrast ceļu uz kontiem, izmēģinot dažas no visbiežāk izmantotajām parolēm – piemēram, 123456 vai pašu vārdu parole. Ja izmantojat kādu no šīm un vēl neesat ticis apdraudēts, iespējams, jums jāiegādājas loterijas biļete, jo esat viens no veiksmīgākajiem cilvēkiem pasaulē;
- **brutāla spēka uzbrukumi**: ja datu pārkāpuma laikā tiek atklāts jūsu lietotājvārds un parole, hakeri var izmantot uzbrukumus, lai atšifrētu jūsu datus. Izmantojot programmu, ir iespējams pārlūkot visas iespējamās paroles (pārbaudot simtiem vai tūkstošiem iespējamo iespēju), līdz izdomā pareizo. Pat ja esat izmantojis lielo un mazo burtu un īpašo rakstzīmju kombināciju, mūsdienu tehnoloģija 8 zīmju paroli var uzlauzt aptuveni divu stundu laikā (!);
- **identifikācijas datu izmantošana vairākās vietās**: Kad hakeriem vai surogātpasta izplatītājiem ir jūsu konta lietotājvārds un parole, viņi var viegli izmēģināt šos identifikācijas datus visos pārējos jūsu kontos. Ja esat izmantojis savus identifikācijas datus vairākās vietās (t.i., izmantojat to pašu lietotājvārdu un paroli citur), jūs teju pasniedzat hakeriem atslēgas uz savu māju – piekļuvi visiem jūsu kontiem, kuriem ir kopīgi šie identifikācijas dati.

1. vingrinājums:  5 - 10 min.

Infografikas izpēte: Pasaulē lielākie datu aizsardzības pārkāpumi un uzlaušanas gadījumi: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Visbiežāk sastopamās kļūdas:

- tā pati parole, bet atšķirīgs profils: "Virginia Tech" datorzinātņu pētījums atklāj, ka 38% cilvēku dažādiem digitālajiem profiliem izmanto vienu un to pašu paroli;
- parole ar nelielu atšķirību: Reģistrējoties jaunās vietnēs, 21% parasti izmanto vienu paroli. Ja paroles maiņai nepieciešams laiks, tiek mainīta tikai neliela daļa;
- parastās paroles: Pētījumi atklāj, ka cilvēki joprojām izmanto, piemēram, "qwerty" vai "123456". Šīs paroles sastāv no labi zināmām burtu un ciparu kombinācijām;
- personīga informācija parolē: Paroles bieži sastāv no jūsu vai radinieka vārda un jubilejas datuma.

(Anon., 2019)

Ir svarīgi izmantot paroles, kuras ir grūti uzminēt un droši uzglabāt.

- Neizmantojiet paroles, kas izveidotas no personvārdiem, adresēm, tālruņa numuriem un citiem vārdiem, kurus var viegli uzminēt.

Izlasiet visbiežāk lietoto paroļu sarakstu un pārbaudiet, vai jūsu parole nav šajā sarakstā: https://nordpass.com/most-common-passwords-list/

Neizpaudiet savu paroli nevienam.

- Atcerieties paroles; nepierakstiet tās uz papīra.

Lasīt rakstu par "lūrēšanu pār plecu": Kas ir lūrēšana pār plecu?

Izvēlieties sarežģītu paroli, kurā ir mazie un lielie burti, cipari un zīmes. Jo garāka ir parole, jo grūtāk to uzminēt.

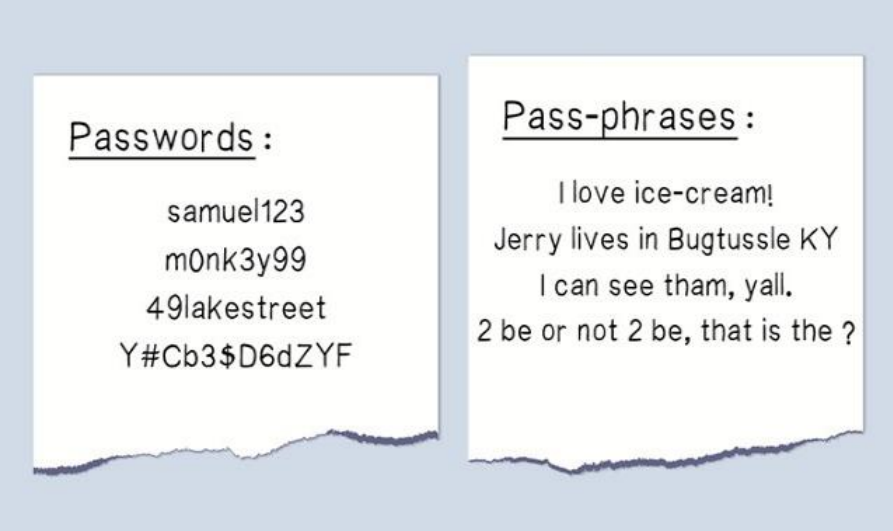
Labākās paroles ir tās, kuras ir:

- viegli atcerēties
- hakeriem grūti uzlaužamas.

Ieejas frāzes veido vislabākās paroles, jo tajās tiek izmantoti reāli vārdi, kurus jūs varat atcerēties (nevis sarežģītu simbolu un burtu kopums), un tās ir ļoti garas, tāpēc tās ir daudz grūtāk uzlauzt ar brutālu spēku uzbrukumiem vai citu taktiku.

(Jonathan Lemonnier; Nica Latto, 2020)

Viens no veidiem, kā viegli atcerēties garas paroles, **ir izmantot frāzes**. Frāze ir teikums ar burtu, ciparu un simbolu kombināciju, ko ir vieglāk atcerēties.



Lai izveidotu **frāzes**, var izmantot:

- vārdi no dziesmas vai dzejoļa;
- citāts no jums svarīgas filmas vai adreses;
- fragments no grāmatas;
- virkne vārdu, kas jums ir svarīgi;
- saīsinājums – izveidojiet paroli no katra teikuma vārda pirmā burta.

2. vingrinājums: 5 - 10 min.

- Pārbaudiet paroles stiprumu, izmantojot tiešsaistes rīku, piemēram: https://howsecureismypassword.net/.
- Izmēģiniet frāžu ģeneratoru: https://www.useapassphrase.com/

Dažādu paroļu izmantošana dažādās vietnēs

Izmantojiet dažādas paroles dažādās vietnēs, jo, ievadot parasto paroli nedrošā vietnē, to var atklāt ļaunprātīgiem cilvēkiem.

Katram kontam ir nepieciešama unikāla parole. Ja izmantojat vienu paroli vairākiem kontiem, jūs pakļaujat sevi lielam riskam. Kiberuzbrucējam ir nepieciešams tikai uzlauzt izmantoto vietni, nozagt visas paroles, ieskaitot jūsu, un pēc tam izmantot paroli, lai pieteiktos visos pārējos kontos. Tas notiek biežāk, nekā jūs domājat. Neticiet tam?

Pārbaudiet adresē www.haveibeenpwned.com, cik no jūsu izmantotajām vietnēm ir uzlauztas, iespējams, apdraudot jūsu paroles.

Periodiski nomainiet paroles

Visi parastie padomi, ko saņemat par parolēm, nav gluži nepareizi. Bet, neieslīgstot tehniskās detaļās (patiesību sakot, vispār nerunājot par tehniskiem jautājumiem), ir tikai divas pamatprasības spēcīgai parolei:

- tai vajadzētu būt garai: patiešām garai. Jūsu parolei jābūt no 10 līdz 20 rakstzīmēm. Lai patiesi nodrošinātos nākotnei, izmantojiet līdz pat 20 rakstzīmēm;
- parolei jābūt nejaušai: hakeri lieliski atpazīst modeļus un ieprogrammē savus rīkus, lai tos meklētu.

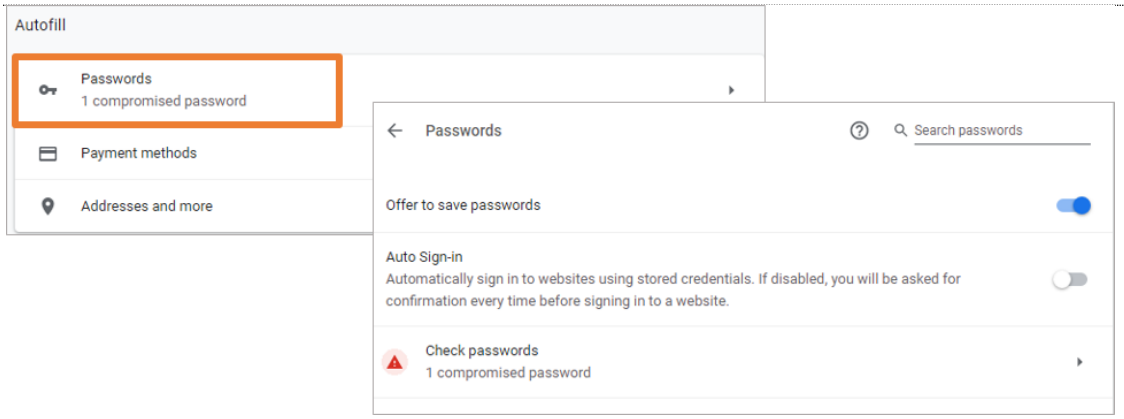
Jūs varat sagatavot spēcīgas paroles, izmantojot tiešsaistes paroļu ģeneratoru: https://passwordsgenerator.net/

Vai ir droši saglabāt paroles?

Neļaujiet pārlūkprogrammai atcerēties jūsu pieteikšanās vārdus un paroles!

Google Chrome piemērs:

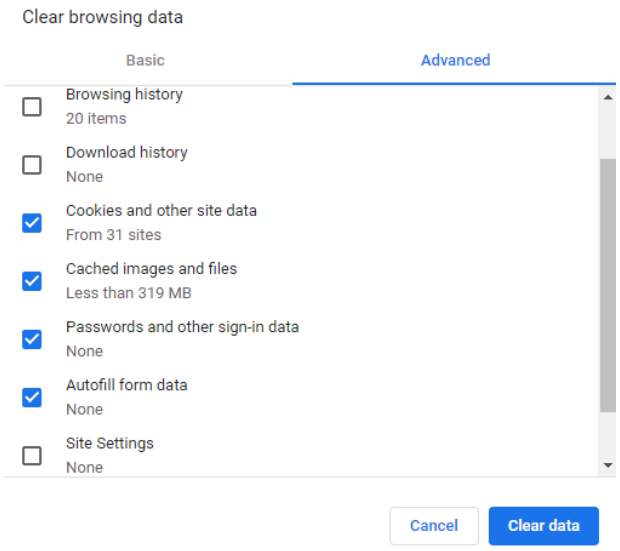
Pretējā gadījumā citi lietotāji varēs izmantot jūsu datus. Dažas pārlūkprogrammas var iestatīt, lai tās atcerētos ievadītos datus nejautājot.



Tāpēc, kad esat pabeidzis darbu, drošības labad izdzēsiet visus privātos datus, kas ievadīti pārlūkprogrammā.

Lai izdzēstu paroles un automātiskās aizpildes datus no pārlūkprogrammas atmiņas, nospiediet taustiņus **CTRL+SHIFT+DELETE.**

Atvērtajā logā atzīmējiet "Paroles un citi pierakstīšanās dati" un noklikšķiniet uz **Notīrīt datus.**



Paroļu pārvaldnieki

Tās ir īpašas lietotnes, kas visas jūsu paroles glabā drošā, šifrētā veidā. Jums ir jāatceras tikai viena parole – paroļu pārvaldniekam. Paroļu pārvaldnieks pēc tam automātiski atrod jūsu paroles attiecīgajās vietnēs, kad jums tās nepieciešams, un jūs autentificē. Tiem ir arī citas funkcijas, piemēram, iespēja saglabāt atbildes uz drošības jautājumiem, brīdināt jūs, ja atkal izmantojat paroli, paroļu ģeneratora funkcija, kas ļaus jums izveidot un izmantot drošas

paroles, un daudzas citas. Lielākā daļa paroļu pārvaldnieku arī droši sinhronizē dažādas ierīces, tāpēc jums ir ērta un droša piekļuve savām parolēm neatkarīgi no izmantotās sistēmas.

Visbeidzot, pierakstiet savu paroļu pārvaldnieka paroli uz papīra un glabājiet to drošā vietā jūsu mājās. Daži paroļu pārvaldnieki ļauj pat izdrukāt paroļu pārvaldnieka atkopšanas rīku. Tātad, ja esat aizmirsis paroļu pārvaldnieka paroli, jums būs rezerves plāns. Vai arī, ja jūs saslimstat vai nonākat slimnīcā, jūsu mīļotais cilvēks vai uzticams ģimenes loceklis varēs iegūt informāciju jūsu vārdā.

Piemēram:

- KEEPER Cybersecurity Starts Here
- LastPass
- bitwarden
- DASHLANE

- 1 parole (Windows, Mac, iOS, Android)
- LastPass (iOS, Android; Chrome spraudņi strādā Windows, Mac, Linux)
- KeePass (Linux, Windows, Mac, Android)

3. vingrinājums: 5 - 10 min.

Lasīt vairāk: https://www.sans.org/security-awareness-training/resources/password-managers-0