Paroļu frāžu izmantošana

Vai ir apnicis pastāvīgi izdomāt sarežģītas paroles? Neapmierina tas, ka jāatceras un jāieraksta visas šīs rakstzīmes, simboli un cipari? Mums ir risinājums: mūžam spēcīgā frāzveida parole!

Frāzveida paroles

Varbūt nemaz neapzināties, bet paroles ir viens no galvenajiem kiberuzbrucēju uzbrukumu vektoriem. Ļaundaru mērķis ir tieši paroles, un, ja viņiem izdodas pareizi uzminēt vai uzlauzt paroli, viņi var viegli piekļūt e-pastam, bankas kontiem vai, iespējams, nozagt visu identitāti. Jo vājākas ir paroles, jo vieglāk ļaundariem ir iegūt piekļuvi. Tāpēc spēcīgas paroles ir viens no efektīvākajiem veidiem, kā aizsargāt kontus un digitālo dzīvi tiešsaistē. Tradicionāli tiek mācīts lietot ļoti sarežģītas paroles. Tika uzskatīts, ka, jo sarežģītāka parole, jo grūtāk kiberuzbrucējiem un viņu automatizētajām programmām to uzminēt. Taču problēma ir tā, ka sarežģītas paroles ir arī grūti gan atcerēties, gan precīzi ievadīt. Vēl labāks veids, kā izveidot spēcīgu un drošu paroli, ir tā sauktā frāzveida parole. Sarežģītības vietā tās ir spēcīgas to garuma dēļ. Lūk, daži piemēri:

Laiks iedzert stipru kafiju!
pazudis-gliemis-pludmale

Frāzveida paroles nav nekas cits kā vārdu virkne, un tās var saturēt vairāk nekā divdesmit rakstzīmes, ja vietne to atļauj. Tas var šķist daudz, taču abos iepriekš minētajos piemēros ir vairāk nekā divdesmit rakstzīmes, un, atšķirībā no parastajām parolēm, frāzveida paroles ir daudz vieglāk atcerēties un vienkāršāk ievadīt. Jo garāka ir frāzveida parole, jo tā ir drošāka. Dažās situācijās var būt nepieciešams frāzveida paroli papildināt ar sarežģītākiem elementiem, t.i., pievienot simbolus, lielos burtus vai ciparus. Vienkāršākais veids, kā to izdarīt, ir aizvietot dažus burtus frāzveida parolē ar simboliem vai cipariem. Piemēram, aizvietojot burtu e ar skaitli 3, iepriekš minētie piemēri kļūst sarežģītāki, taču joprojām ir pietiekami viegli atcerēties un ievadīt:

Laiks i3dz3rt stipru kafiju!
pazudis-gliemis-pludmal3

Neatkārtojies

Lai frāzveida parole būtu patiesi droša, tai ir jābūt unikālai katram kontam. Ja vairākos kontos atkārtoti tiek izmantota viena un tā pati frāzveida parole vai frāzveida parole ar viegli atpazīstamu raksturu, jūs pakļaujat sevi briesmām.

Kiberuzbrucējam pietiek uzlauzt vienu no bieži izmantotajām vietnēm, nozagt paroli, ko izmantojat šai konkrētajai vietnei, un, ja visas paroles/frāzveida paroles ir vienādas, varēs piekļūt pārējiem kontiem. Nespējat atcerēties visas šīs garās, unikālās frāzveida paroles katram kontam? Mums ir risinājums: paroļu pārvaldnieki.

Paroļu pārvaldnieki ir īpašas datorprogrammas, kas visas paroles droši glabā šifrētā glabātavā, kuru aizsargā primārā parole. Lai piekļūtu glabātavai, jāatceras tikai primārā parole. Paroļu pārvaldnieks var automātiski izgūt paroles, kad vien tās ir nepieciešamas, un automātiski pieslēgties vietnēm jūsu vietā. Paroļu pārvaldnieki ir attīstījušies, ietverot arī citas funkcijas, tostarp atbilžu uz slepeniem jautājumiem glabāšanu, brīdināšanu, ja atkārtoti izmantojat paroles vai nokļūstat viltus tīmekļa vietnē, ģeneratoru izmantošanu, kas jūsu vietā izveido spēcīgas paroles vai frāzveida paroles, un daudzas citas funkcijas. Lielākā daļa paroļu pārvaldnieku arī droši sinhronizējas gandrīz jebkurā datorā vai ierīcē, tāpēc neatkarīgi no tā, kādu sistēmu izmantojat, tā ir ērta un droša piekļuve visām jūsu parolēm.

Pēdējais solis – daudzfaktoru autentifikācija

Pēdējais solis, kā padarīt frāzveida paroles patiesi drošas, ir pievienot tām otru aizsardzības līmeni, ko sauc par daudzfaktoru autentifikāciju (MFA). MFA pieprasa, lai, pieslēdzoties kontiem, jums būtu divi identifikācijas elementi. Tie var būt parole un biometriskie dati, piemēram, pirkstu nospiedums, vai arī parole un automātiski ģenerēts ciparu kods, kas tiek nosūtīts uz citu ierīci vai e-pastu. Šis kods katru reizi ir unikāls, un to var ģenerēt no mobilā tālruņa vai citas uzticamas ierīces. Šis process nodrošina, ka pat tad, ja kiberuzbrucējs iegūst jūsu paroli, viņš joprojām nevarēs piekļūt jūsu kontiem, jo viņam nav otrā faktora. MFA būtu jāaktivizē, kad vien iespējams, jo īpaši svarīgākajiem kontiem, piemēram, bankas, pensijas vai personīgā e-pasta kontiem. Ja izmantojat paroļu pārvaldnieku, ir ļoti ieteicams to aizsargāt ar spēcīgu frāzveida paroli UN daudzfaktoru autentifikāciju.

Frāzveida paroles ir lielisks veids, kā gan vienkāršot drošību, gan palīdzēt aizsargāt kontus. Lai padarītu digitālo dzīvi tiešsaistē vēl vienkāršāku un drošāku, iesakām kombinēt paroļu pārvaldnieku un daudzfaktoru autentifikācijas iespējas frāzveida parolēm.

Viesredaktors

Kvintana Patersone (Quintana Patterson) ir Kolorādo Universitātes Anšutzas medicīnas pilsētiņas (University of Colorado Anschutz Medical Campus) IT klīniskās un atbilstības nodrošināšanas vadītāja un WiCyS (Sievietes kiberdrošībā) (Women in CyberSecurity) Līdztiesību aizstāvības komitejas priekšsēdētāja. Viņa ir apņēmusies nodrošināt, lai sievietes šajā nozarē justos gaidītas, atbalstītas un novērtētas.

Resursi

Paroļu pārvaldnieki: https://www.sans.org/newsletters/ouch/password-managers/
Biometrija: https://www.sans.org/newsletters/ouch/biometrics-making-security-simple/
Vairāku faktoru autentifikācija: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/

Tulkojums: CERT.LV