OUCH!

SANS SECURITY AWARENESS

Ikmēneša Informācijas drošības izdevums Tev

Kā padarīt paroles vieglāk iegaumējamas

Pārskats

Jums bieži tiek teikts, ka jūsu izvēlētās paroles ir svarīgākais un primārais "vairogs" jūsu kontu aizsardzībai (kas tā arī ir!), bet reti jums tiek piedāvāts vienkāršs veids, kā droši izveidot un uzglabāt visas jūsu paroles. Zemāk aplūkosim trīs vienkāršus soļus, kā vienkāršot paroles, pasargāt jūsu kontus un nosargāt jūsu nākotni.

Paroļu frāzes

Trako, sarežģīto paroļu laiks ir cauri. Šīs paroles ir grūti atcerēties, sarežģīti ierakstīt, un ar mūsdienu super-ātrajiem datoriem kibernoziedznieki tās var viegli uzlauzt. Paroļu svarīgākā īpašība – tām jābūt garām, jo vairāk simbolu ir parolē, jo labāk. Tās sauc par paroļu frāzēm, tas ir drošu paroļu veids, kurā izmanto īsus teikumus vai gadījuma vārdus. Daži piemēri:

Laiks stiprai melnai kafijai!

pazudis-gliemezis-lien-pludmale

Abas ir drošas, ar vairāk kā 20 simboliem, abas ir viegli atcerēties un vienkārši uzrakstīt, bet grūti uzlauzt. Jūs saskarsieties ar tīmekļa vietnēm vai situācijām, kurās tiks prasīts parolē izmantot simbolus, ciparus vai lielos burtus, arī tā var. Bet atcerieties, ka galvenais parolē ir garums!

Paroļu pārvaldnieki

Jums nepieciešama unikāla parole katram jūsu kontam. Ja izmantojat vienu paroli vairākiem kontiem, jūs pakļaujat sevi lielam riskam. Viss, kas kiberuzbrucējam ir nepieciešams, ir uzlauzt jūsu izmantoto tīmekļa vietni, nozagt visas paroles, ieskaitot jūsējo, un tad izmantot jūsu paroli, lai autorizētos visos citos jūsu kontos. Tas notiek biežāk nekā jūs to iedomājaties. Neticiet? Pārbaudiet www.haveibeenpwned.com cik daudzas vietnes, kuras izmantojat, ir tikušas uzlauztas, un, iespējams, jūsu paroles kompromitētas. Ko tad darīt? Izmantot paroļu pārvaldnieku.

Tās ir speciālas datorprogrammas, kas glabā visas jūsu paroles drošā, šifrētā veidā. Jums jāatceras tikai viena parole - jūsu paroļu pārvaldniekam. Paroļu pārvaldnieks pēcāk automātiski sameklē jūsu paroles atbilstošajām vietnēm, kad jums tas ir nepieciešams, un autentificē jūs. Tiem ir vēl arī citas funkcijas, piemēram, iespēja saglabāt jūsu atbildes uz drošības jautājumiem,

brīdināt jūs, ja izmantojat paroli atkārtoti, paroļu ģeneratora funkcija, kas ļaus jums veidot un izmatot drošas paroles, un daudzas citas iespējas. Lielākā daļa paroļu pārvaldnieku arī droši sinhronizējas starp virkni dažādu ierīču, tā ka jums ir vienkārša un droša piekļuve jūsu parolēm, neatkarīgi no tā, kādu sistēmu jūs izmantojat.

Visbeidzot, pierakstiet sava paroļu pārvaldnieka paroli uz papīra un noglabājiet to drošā vietā savās mājās. Daži paroļu pārvaldnieki pat ļauj izdrukāt paroļu pārvaldnieka atgūšanas rīku. Tādejādi, ja jūs aizmirsīsiet sava paroļu pārvaldnieka paroli, jums būs rezerves plāns. Vai arī, ja paliksiet slims vai tiksiet hospitalizēts, jūsu otrā puse vai uzticams ģimenes loceklis varēs jūsu vārdā iegūt informāciju.

Divu faktoru autentifikācija

Divu soļu verifikācija (bieži saukta arī par divu faktoru autentifikāciju vai daudzfaktoru autentifikāciju) sniedz papildus drošības līmeni. Tā pieprasa divas lietas, kad veicat pierakstīšanos savos kontos, jūsu paroli un ciparu kodu, kurš tiktu uzģenerēts jūsu viedierīcē vai atsūtīts uz jūsu telefonu. Šis process nodrošina to, ka pat tad, ja kiberuzbrucēji ir ieguvuši jūsu paroles, tie nevar piekļūt jūsu kontiem. Divu faktoru autentifikācija ir vienkārši uzstādāma, un parasti jums to jāizmanto tikai vienreiz, kad veicat autorizāciju no jaunas iekārtas. Iespējojiet to, kad vien iespējams, it īpaši saviem svarīgākajiem kontiem, tādiem kā jūsu banka vai e-pasts. Ja jūs izmantojat paroļu pārvaldnieku, mēs ļoti iesakām to aizsargāt gan ar drošu paroļu frāzi, gan ar divu faktoru autentifikāciju.

Tas var izklausīties muļķīgi, bet šie trīs vienkāršie soļi sniedz nozīmīgu atbalstu jūsu darba, jūsu reputācijas un jūsu finansiālās nākotnes aizsargāšanā.

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

Justin Henderson *(@SecurityMapper) ir H & A Security Solutions līdzdibinātājs, sertificēts SANS institūta instruktors un SANS kiberaizsardzības un SIEM kursu autors. Viņam patīk viss, kas saistīts ar kiberaizsardzību, un viņš konsultē jau piecpadsmit gadus.*

Resursi

Have I Been Pwned:	https://haveibeenpwned.com/
Divu faktoru autentifikācija:	https://twofactorauth.org/
NIST SP800-63B digitālās identitātes vadlīnijas:	https://pages.nist.gov/800-63-3/sp800-63b.html
Plakāts: Tu esi mērķis:	https://www.sans.org/u/OGi

Redakcija: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Tulkojums: Līga Besere