SANS SECURITY AWARENESS

Vaš mesečni bilten za podizanje svesti o bezbednosti informacija

Menadžeri lozinki

Uvod

Jedan od najvažnijih koraka koje možete preduzeti kako biste se zaštitili je da koristite jedinstvenu i jaku lozinku za svaki vaš nalog i aplikaciju. Nažalost, skoro da je nemoguće zapamtiti sve te različite lozinke. Pritom, ručno unošenje lozinki na različitim sajtovima, kreiranje novih lozinki, staranje o odgovorima na bezbednosna pitanja i brojnim drugim aspektima predstavljaju vremenski zahtevne aktivnosti. Međutim, postoji rešenje koje će vam život učiniti mnogo jednostavnijim i daleko bezbednijim. To su menadžeri lozinki.

Kako rade menadžeri lozinki

Menadžeri lozinki rade tako što čuvaju sve vaše lozinke u bazi podataka, koja se ponekad naziva i sef. Menadžer lozinki šifruje sadržaj baze i štiti ga pomoću glavne lozinke koju znate samo vi. Kada vam je potrebna neka od vaših lozinki, npr. da biste se prijavili na vaš nalog za finansijske usluge (e-banking) ili elektronsku poštu, potrebno je samo da unesete vašu glavnu lozinku u menadžer lozinki kako biste otključali bazu (sef). Menadžer lozinki će automatski izvući odgovarajuću lozinku i bezbedno vas prijaviti na željeni veb sajt. To znači da ne morate više da pamtite vaše lozinke niti da ručno unosite kredencijale za pristup.

Pored navedenog, većina menadžera lozinki ima i mogućnost automatske sinhronizacije na više različitih uređaja. Stoga će se, kada ažurirate lozinku u menadžeru na vašem laptopu, te promene odraziti i na sve vaše druge uređaje. Konačno, većina menadžera lozinki prepoznaje kada kreirate novi nalog na internetu ili ažurirate lozinku postojećeg naloga, te automatski ažuriraju sef za vas.

Od izuzetne je važnosti da glavna (master) lozinka koju koristite za zaštitu menadžera lozinki bude dugačka i jedinstvena. Zbog toga se preporučuje da glavnu lozinku napravite kao pristupnu frazu - dugačku lozinku sastavljenu od nekoliko reči ili fraza. Ukoliko vaš menadžer lozinki podržava dvofaktorsku autentifikaciju, obavezno je koristite. Na kraju, budite sigurni da ste zapamtili vašu glavnu lozinku. U slučaju da je zaboravite, nećete moći da pristupite drugim lozinkama koje čuvate u menadžeru lozinki.

Izbor menadžera lozinki

Postoji veliki izbor menadžera lozinki. U odeljku Dodatni materijal dat je link na jedan pregled menadžera lozinki. Dok budete tražili najbolje rešenje za vas, vodite računa i o sledećem:

Vaš menadžer lozinki treba da bude jednostavan za korišćenje. Ako vam je odabrano rešenje suviše složeno za razumevanje, pronađite drugo koje više odgovara vašim navikama i veštinama.

Menadžer lozinki treba da radi na svim uređajima na kojima upotrebljavate lozinke. Takođe, treba da ima mogućnost jednostavne sinhronizacije lozinki između svih vaših uređaja.

Koristite samo dobro poznate i pouzdane menadžere lozinki. Budite obazrivi prema rešenjima koja su nova na tržištu ili o kojima ima malo povratnih informacija korisnika. Sajber kriminalci mogu da naprave lažne menadžere lozinki kako bi vam ukrali informacije. Takođe, budite veoma obazrivi u slučajevima kada proizvođači tvrde da su razvili svoje rešenje za enkripciju.

Izbegavajte one menadžere lozinki za koje proizvođač tvrdi da može da vam oporavi vašu glavnu lozinku. To znači da oni znaju vašu glavnu lozinku, što vas izlaže visokom riziku.

Koje god rešenje da ste odabrali, uverite se da ga proizvođač kontinuirano ažurira i izdaje ispravke i postarajte se da uvek koristite najnoviju verziju.

Menadžer lozinki treba da omogućava čuvanje i drugih osetljivih podataka, kao što su odgovori na vaša tajna bezbednosna pitanja, podaci o platnim karticama, brojevi vaših kartica lojalnosti.

Razmotrite da vašu glavnu lozinku čuvate u zatvorenoj koverti smeštenoj u zaključanom ormanu, metalnom sefu ili kutiji koja se zaključava.

Menadžeri lozinki su odličan način za bezbedno čuvanje svih vaših lozinki i drugih osetljivih podataka, poput brojeva platnih kartica. Međutim, njihova bezbednost i dalje zavisi od vas samih te je neophodno da uvek koristite jedinstvenu i jaku glavnu lozinku, kao i najnoviju verziju odabranog rešenja.

Verzija na srpskom

Telekom Srbija kao društveno odgovorna telekomunikaciona kompanija pomaže prevođenje i distribuciju ovog biltena kako bi se unapredila svest korisnika informaciono-komunikacionih tehnologija o bezbednosti informacija.

Gost urednik

Rasel Jubanks *je lider u oblasti bezbednosti informacija. Živi u Atlanti, ima preko 20 godina iskustva i poseduje mnoge sertifikate iz ovog domena bezbednosti. Rukovodilac je SANS Internet Storm centra i saradnik na polju Kritičnih bezbednosnih kontrola (eng. Critical Security Controls). Možete ga pronaći na @russelleubanks i https://www.securityeverafter.com.*

Dodatni materijal

Napravite lozinku na jednostavan način: http://www.sans.org/u/10Uu

Digitalna zaostavština: http://www.sans.org/u/10Uz

Pregled najboljih menadžera lozinki na Wired portalu: https://www.wired.com/story/best-password-managers/