
OUCH!

SANS SECURITY AWARENESS

Vaš mesečni bilten za podizanje svesti o bezbednosti informacija

# Napravite lozinku na jednostavan način

## Uvod

Sigurno stalno slušate savete kako su vaše lozinke ključ za zaštitu vaših naloga (što je tačno!), ali retko dobijete jednostavnu preporuku kako da bezbedno kreirate i upravljate svim vašim lozinkama. U tekstu u nastavku navedena su tri prosta koraka da pojednostavite vaše lozinke, obezbedite vaše naloge i zaštitite vašu budućnost.

## Fraze za pristup

Vreme neobičnih, komplikovanih lozinki je prošlost. Te lozinke su teške za pamćenje, komplikovane za kucanje, a sa današnjim super brzim računarima sajber napadači ih relativno lako provale. Ključno za lozinke je da budu dugačke, što više karaktera imaju to bolje. Ovakav tip jakih lozinki u kojima se koriste kratke rečenice ili nasumice izabrane reči poznat je pod imenom pristupne fraze ili samo fraze. U nastavku su kao ilustracija data dva primera fraza za pristup:

*Vreme je za jaku kafu!*
*Izgubljeni-puž-puzi-plažom*

Obe ove lozinke su jake sa više od dvadeset karaktera dužine, lako se pamte i jednostavno unose, ali su teške za provaljivanje. Iako ćete naići na veb sajtove ili situacije u kojima se traži da u vašu lozinku dodate simbole, brojeve ili velika slova, što je sasvim legitiman zahtev, zapamtite da je za lozinku najvažnija njena dužina.

## Menadžeri lozinki

Potrebna vam je jedinstvena lozinka za svaki nalog. Ako koristite istu lozinku za više naloga, dovodite sebe u veliku opasnost. Sve što sajber napadač treba da uradi je da hakuje vebsajt koji koristite, ukrade sve lozinke uključujući vašu, i onda iskoristi vašu lozinku da bi se prijavio na sve vaše naloge kao vi. Ovo se dešava mnogo češće nego što pretpostavljate. Ne verujete? Na veb sajtu www.haveibeenpwned.com možete proveriti koji su sajtovi od onih koje koristite hakovani a vaše lozinke potencijalno kompromitovane. Dakle, šta treba da preduzmete? Koristite menadžer lozinki.

Menadžer lozinki je specijalizovani računarski program koji bezbedno čuva sve vaše lozinke u kriptovanoj bazi podataka, sefu. Vi onda samo treba da zapamtite jednu lozinku, onu za vaš menadžer lozinki koji automatski povlači vaše lozinke kada su vam

potrebne i prijavljuje se na veb sajtove umesto vas. Menadžeri lozinki takođe imaju dodatne funkcionalnosti poput čuvanja odgovora na vaša bezbednosna pitanja, upozoravanja kada koristite iste lozinke, generatora lozinki koji osigurava da koristite jake lozinke i mnogih drugih. Većina menadžera lozinki se bezbedno sinhronizuje između bilo kog računara ili uređaja, tako da bez obzira koji sistem koristite imate jednostavan i bezbedan pristup svim vašim lozinkama.

Konačno, obavezno zapišite lozinku za vaš menadžer lozinki i čuvajte je na sigurnom mestu kod kuće. Neki menadžeri lozinki vam čak dozvoljavaju da odštampate komplet za oporavak menadžera lozinki. Time se osigurava da čak i ako zaboravite lozinku za vaš menadžer lozinki imate način da pristupite svojim lozinkama. Ovo je važno i u slučaju da se razbolite ili se nađete u hitnoj situaciji, jer će vaši članovi porodice moći da izvuku informacije umesto vas.

## Verifikacija u dva koraka

Verifikacija u dva koraka (često se naziva i dvofaktorska ili multifaktorska autentifikacija) dodaje još jedan nivo zaštite. Ovaj vid autentifikacije zahteva od vas da imate dve stvari kada se prijavljujete na svoje naloge, lozinku i numerički kod koji generiše vaš pametni telefon ili vam se šalje na telefon. Ovaj postupak osigurava da čak i slučaju da sajber napadač sazna vašu lozinku on se i dalje ne može prijaviti na vaše naloge. Verifikacija u dva koraka je jednostavna za podešavanje i obično se zahteva da je upotrebite samo jedanput kada se prijavljujete sa novog računara ili uređaja. Omogućite verifikaciju u dva koraka kad god je ta opcija na raspolaganju, posebno za najvažnije naloge kao što su vaši bankovni računi ili nalozi za pristup elektronskoj pošti. Ako koristite menadžer lozinki, obavezno ga zaštitite pomoću jake pristupne fraze i verifikacije u dva koraka.

Možda zvuči neverovatno, ali ova tri jednostavna koraka će vam na duge staze zaštititi posao, ugled i finansijsku budućnost.

## 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

***Džastin Henderson*** *(@SecurityMapper) je suosnivač kompanije „H&A Security Solutions“, sertifikovani SANS instruktor i autor SANS-ovih kurseva o sajber odbrani i SIEM-u. Džastin voli sve što je u vezi sa sajber zaštitom, a konsultantskim poslom se bavi već 15 godina unazad.*

## Dodatni materijal

| | |
|---|---|
| Veb sajt: Da li mi je ukradena lozinka: | https://haveibeenpwned.com/ |
| Veb sajt: Dvofaktorska autentifkacija: | https://twofactorauth.org/ |
| Standard: NIST SP800-63B Smernice za digitalni identitet: | https://pages.nist.gov/800-63-3/sp800-63b.html |
| Poster: Vi ste meta: | https://www.sans.org/u/OGi |