SANS Telekom Srbija

OUCH! | April 2017

Mesečni bilten za podizanje svesti o bezbednosti informacija

OUCH!

U OVOM BROJU...

- **Pristupne fraze (passphrases)**
- **Bezbedno korišćenje fraza**
- **Dodatni materijal**

Pristupne fraze

Uvod

Lozinke gotovo svakodnevno koristite, počev od pristupa elektronskoj pošti ili online bankarskim uslugama do kupovine robe i pristupa mobilnom telefonu. Samim tim, lozinke su jedna od vaših najslabijih tačaka, jer ako neko sazna ili pogodi vašu lozinku on može da pristupi vašim nalozima, obavlja transakcije vašim novcem, čita vašu elektronsku poštu ili ukrade vaš identitet. To je razlog zbog koga su jake lozinke ključne za vašu zaštitu. Međutim, lozinke često zbunjuju korisnike, teško se pamte i unose. U ovom broju saznaćete kako da kreirate jake lozinke koje su lake za pamćenje i jednostavne za unos, poznate kao pristupne fraze (passphrases) ili samo fraze.

Gost urednik

My-Ngoc Nguyen je sertifikovana SANS instruktorka i direktorka/glavni konsultant u kompaniji „Secured IT Solutions“. Poseduje vrhunske sertifikate i ima preko 14 godina iskustva u razvoju, unapređenju i upravljanju programima na polju sajber bezbednosti u različitim oblastima. Twitter: **@MenopN** LinkedIn: My-Ngoc “Menop” Nguyen.

Pristupne fraze (passphrases)

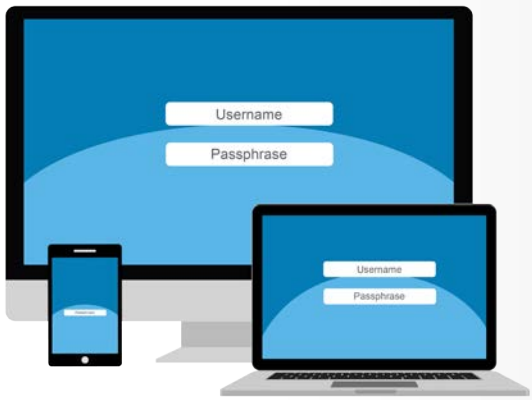
Pretnja sa kojom se svi susrećemo je činjenica da su sajber kriminalci razvili sofisticirane i efikasne metode za otkrivanje lozinki, automatizujući proces pogađanja lozinki, tzv. bruteforce napade. To znači da oni mogu da otkriju vaše lozinke ukoliko su one slabe ili lake za pogađanje. Da biste se zaštitili važno je da koristite jake lozinke. To u praksi obično znači kreiranje kompleksnih lozinki, međutim, one se teško pamte, često zbunjuju korisnike i teško se unose. Umesto toga preporučujemo vam korišćenje fraza, niza slučajnih reči ili rečenice. Što više karaktera vaše fraze sadrže, one su jače. Njihova prednost je u tome što se mnogo lakše pamte i unose, dok je istovremeno sajber napadačima teško da ih hakuju. Dva takva primera su:

LidoJeNaVelikomRatnomOstrvu
Radnim danom ustajem u 6:15

Ono što ove pristupne fraze čini jakim nije samo činjenica da su duge, već i činjenica da se koriste velika slova i specijalni znaci (razmak i znaci interpunkcije su specijalni znaci). U isto vreme ove fraze su lake za pamćenje i unos. Fraze možete učiniti još jačim ako pojedina slova zamenite brojevima ili specijalnim znacima, na primer slovo „a“ možete zameniti znakom „@“, a

Pristupne fraze

slovo „o“ nulom. Ako veb sajt ili aplikacija ograničavaju broj karaktera koji lozinka može da ima, koristite maksimalni dozvoljeni broj karaktera.



Fraze su jednostavniji način za kreiranje i pamćenje jakih lozinki.

Bezbedno korišćenje fraza

Prilikom korišćenja fraza neophodno je da budete oprezni, jer vam one neće biti od koristi ako ih neko može lako ukrasti ili kopirati.

1. Koristite različite fraze za svaki nalog ili uređaj koji koristite. Na primer, nikada ne koristite istu frazu za vaš korisnički nalog na poslu ili bankovni račun i za svoje privatne naloge na Facebook-u, YouTube-u ili Twitter-u. Na taj način, ako je jedan od vaših naloga kompromitovan, ostali će i dalje biti bezbedni. Ako koristite veliki broj fraza koje je potrebno zapamtiti (što je veoma čest slučaj), razmotrite upotrebu menadžera lozinki. To je specijalni program za bezbedno čuvanje svih vaših fraza i lozinki, i u tom slučaju su jedine fraze koje ćete morati da zapamtite one za pristup vašem računaru ili uređaju i za pristup menadžeru lozinki.
2. Nikada ne delite sa drugima (uključujući vaše kolege ili nadređenog) svoje fraze ili strategiju za njihovo kreiranje. Imajte na umu da fraza treba da bude tajna, a ako je neko drugi zna ona to više nije. Ako ste slučajno podelili frazu sa nekim, ili sumnjate da je ona kompromitovana ili ukradena, odmah je promenite. Jedni izuzetak je slučaj kada želite da svoje najvažnije lične fraze podelite sa članom porodice kome zaista verujete, ali sa idejom da se koriste u hitnim situacijama. Jedan način da ovo učinite je da zapišete vaše najvažnije lične pristupne fraze (postarajte se da nisu vezane za posao), smestite ih na sigurno mesto i podelite informaciju o toj lokaciji sa tim članom porodice. Na taj način, u slučaju da vam se nešto desi i da vam je potrebna pomoć, osoba od poverenja će moći da pristupi vašim važnim nalozima.
3. Nemojte koristiti javne računare, kao što su oni u hotelima ili Internet kafeima, za prijavljivanje na vaše naloge. Pošto takve računare može da koristi bilo ko, oni mogu biti zaraženi malicioznim softverom koji snima sve što je na tastaturi otkucano. Za prijavljivanje na vaše naloge koristite samo pouzdane računare ili mobilne uređaje.
4. Budite pažljivi sa veb sajtovima koji zahtevaju da odgovorite na lična pitanja. Ova pitanja se koriste u slučaju da ste zaboravili vašu frazu i potrebno je da je ponovo postavite (resetujete). Problem je što se odgovori na ova pitanja često mogu naći na Internetu ili na vašoj Facebook strani. Pobrinite se da u odgovorima na lična pitanja koristite samo informacije koje nisu javno dostupne ili su fiktivni podaci koje ste izmislili. Ne možete da zapamtite sve te odgovore

na bezbednosna pitanja? Odaberite temu poput lika iz filma i bazirajte vaše odgovore na tom liku. Druga opcija je da koristite menadžere lozinki jer većina ovih alata omogućava da se na bezbedan način čuvaju i ove dodatne informacije.

5. Veliki broj veb sajtova nudi mogućnost korišćenja dvofaktorske autentifikacije (verifikacije iz dva koraka). U tom slučaju se prilikom autentifikacije traži još nešto osim fraze, na primer kod za pristup (šifra) poslat na vaš mobilni telefon. Ovakav način autentifikacije je daleko bezbedniji od korišćenja samo pristupne fraze. Kad god je to moguće, omogućite i koristite takve metode autentifikacije.
6. Mobilni uređaji često traže unos PIN-a u cilju zaštite pristupa. Imajte na umu da je PIN takođe jedna vrsta lozinke. Što je PIN duži, to je bezbedniji. Mnogi mobilni uređaji dozvoljavaju korišćenje fraze umesto PIN-a ili korišćenje biometrije poput otiska prsta.
7. Na kraju, ako više ne koristite neki nalog, obavezno ga treba zatvoriti, obrisati ili onemogućiti njegovo dalje korišćenje.

Saznajte više

Prijavite se na OUCH! mesečni bilten za podizanje svesti o bezbednosti informacija namenjen svima, pročitajte prethodne brojeve OUCH!-a i saznajte više o SANS-ovim rešenjima za unapređenje svesti o bezbednosti informacija na našoj internet prezentaciji securingthehuman.sans.org/ouch/archives.

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.

Dodatne informacije

Menadžeri lozinki:	https://securingthehuman.sans.org/ouch/2015#october2015
Verifikacija iz dva koraka:	https://securingthehuman.sans.org/ouch/2015#september2015
Obezbedite vaš pristup:	https://lockdownyourlogin.com
SANS SEC301 – petodnevna obuka o osnovama sajber bezbednosti:	https://sans.org/sec301

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Кэти Клик, Cheryl Conley
Preveli: Dragan Ristić i Gordana Živanović