SANS SECURITY AWARENESS
Telekom Srbija
OUCH! | Decembar 2017
Mesečni bilten za podizanje svesti o bezbednosti informacija

OUCH!

U OVOM BROJU...

- Lozinke
- Šta je dvofaktorska autentifikacija
- Kako funkcioniše

Obezbedite svoj nalog

Uvod

Proces autentifikacije ili utvrđivanja identiteta ključan je za zaštitu vaših informacija poput elektronske pošte, informacija na društvenim mrežama ili onlajn bankovnim računima. Možda niste svesni ali postoje tri različita načina da dokažete ko ste: pomoću nečega što znate - kao što je lozinka, nečega što imate - kao što je vozačka dozvola i nečega što je deo vas samih - poput otiska prsta. Svaka od ovih metoda ima prednosti i mane. Najčešće se kao metod autentifikacije koriste lozinke, dakle nešto što znate. Nažalost, sve se više pokazuje da korišćenje samo lozinki nije dovoljno bezbedno. U ovom tekstu možete saznati kako da zaštitite sebe i svoje naloge nečim što je bolje od samih lozinki, a zove se dvofaktorska autentifikacija.

Gost urednik

Tifani Šonike je direktorka za kampanje i inicijative pri Nacionalnoj alijansi za sajber bezbednost (**@staysafeonline**). Tokom 2016. godine, u saradnji sa Belom kućom, vladom SAD i različitim industrijama, radila je na kampanji pod imenom STOP. THINK. CONNECT.™ koja se bavila i povećavanjem bezbednosti naloga i dvofaktorskom autentifikacijom.

Lozinke više nisu dovoljne

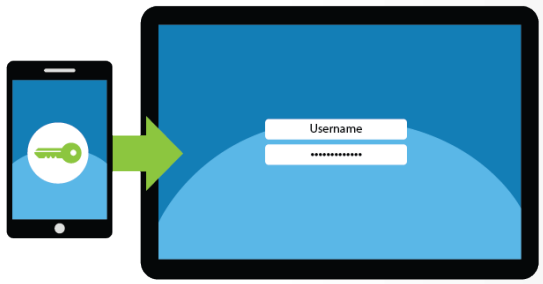
Lozinke dokazuju ko ste na osnovu nečega što vi znate. Međutim, ako neko uspe da pogodi ili pristupi vašoj lozinki, on može da se predstavi kao vi i pristupi svim vašim informacijama. Kompromitovane lozinke postale su jedan od glavnih uzročnika hakovanja naloga. Otud i saveti da kad kreirate lozinke koristite fraze koje će drugi teško moći da pogode, da koristite različite lozinke za svaki vaš nalog i da nikada ne delite svoje lozinke sa drugima. Iako svi ovi saveti ostaju na snazi, činjenica je da lozinke više nisu uspešan metod zaštite. Srećom, postoji lak i brz način da opet uspostavite kontrolu i učinite svoje lične informacije bezbednijim, a to je dvofaktorska autentifikacija.

Šta je dvofaktorska autentifikacija?

Dvofaktorska autentifikacija (dvostepena verifikacija, verifikacija iz dva koraka, multifaktorska autentifikacija, 2FA) je daleko bezbednija nego autentifikacija prilikom koje se koriste samo lozinke. Funkcioniše tako što zahteva ne jednu već dve

Obezbedite svoj nalog

različite metode za dokazivanje da ste vi osoba za koju se predstavljate. Dobar primer je vaša platna kartica. Kada podižete novac na bankomatu, vi zapravo koristite dvofaktorsku autentifikaciju. Da biste podigli svoj novac potrebe su vam dve stvari, vaša platna kartica (nešto što imate) i vaš PIN (nešto što znate). Ako izgubite ili vam neko ukrade platnu karticu niko drugi ne može da podigne vaš novac bez poznavanja PIN-a. Kradljivac mora da ima i vašu platnu karticu i PIN da bi na bankomatu obavio transakciju. Dvofaktorska autentifikacija koristi isti koncept.



Obezbedite svoj nalog korišćenjem dvofaktorske autentifikacije kad god je to moguće, jer je to jedan od najvažnijih koraka za zaštitu na internetu koji možete da preduzmete.

Kako funkcioniše

Dvofaktorska autentifikacija je široko rasprostranjena na većini sajtova poznatih banaka, usluga e-pošte, društvenih mreža i drugih. Osim toga većina ovih sajtova nudi i jednostavna uputstva korak-po-korak za omogućavanje dvofaktorske autentifikacija (više informacija naći ćete na kraju u odeljku Dodatne informacije). Jednom kada omogućite dvofaktorsku autentifikaciju možete da očekujete da funkcioniše na sledeći način. Prvo, svom nalogu pristupate korišćenjem korisničkog imena i lozinke kao što ste to i ranije činili. Time ste upotrebili prvi od dva faktora – nešto što znate. Zatim će vam, najčešće putem tekstualne poruke na mobilni telefon, biti poslat jedinstveni kod (da biste primili kod morate da imate svoj telefon). Jedinstveni kod unosite u polje na stranici za prijavljivanje i time ste upotrebili i drugi od dva faktora. Tako je vaš nalog dodatno obezbeđen. Čak i ako sajber kriminalac ukrade vašu lozinku, neće moći da pristupi vašem nalogu osim ako nema i vaš telefon.

Umesto korišćenja jedinstvenog koda dobijenog putem tekstualne poruke, možete na vašem pametnom telefonu da instalirate posebnu mobilnu aplikaciju za autentifikaciju. Aplikacija neprestano generiše novi jedinstveni kod koji možete da upotrebite kad god poželite da se prijavite. Prednost mobilne aplikacije je u još većoj bezbednosti jer se jedinstveni kod generiše u aplikaciji umesto da se prenosi mobilnom mrežom kao tekstualna poruka. Pored toga, zgodnija je za upotrebu jer nije neophodno da budete povezani na mobilnu mrežu kako biste dobili vaš jedinstveni kod.

Obezbedite svoj nalog

Iako na prvi pogled možda deluje da dvofaktorska autentifikacija zahteva mnogo posla, njenim korišćenjem će vaše lične informacije biti znatno bezbednije. Ne čekajte da vaši nalozi budu kompromitovani, već za vaše važne naloge poput naloga za e-poštu, bankovnih ili naloga na društvenim mrežama omogućite upotrebu dvofaktorske autentifikacije i budite spokojni znajući da su mnogo bezbedniji.

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

Pristupne fraze:	https://securingthehuman.sans.org/ouch/2017#april2017
Sajtovi koji podržavaju dvofaktorsku autentifikaciju:	https://twofactorauth.org
Stop|Think|Connect:	https://www.lockdownyourlogin.org
Google dvostepena verifikacija:	http://www.google.com/landing/2step/

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