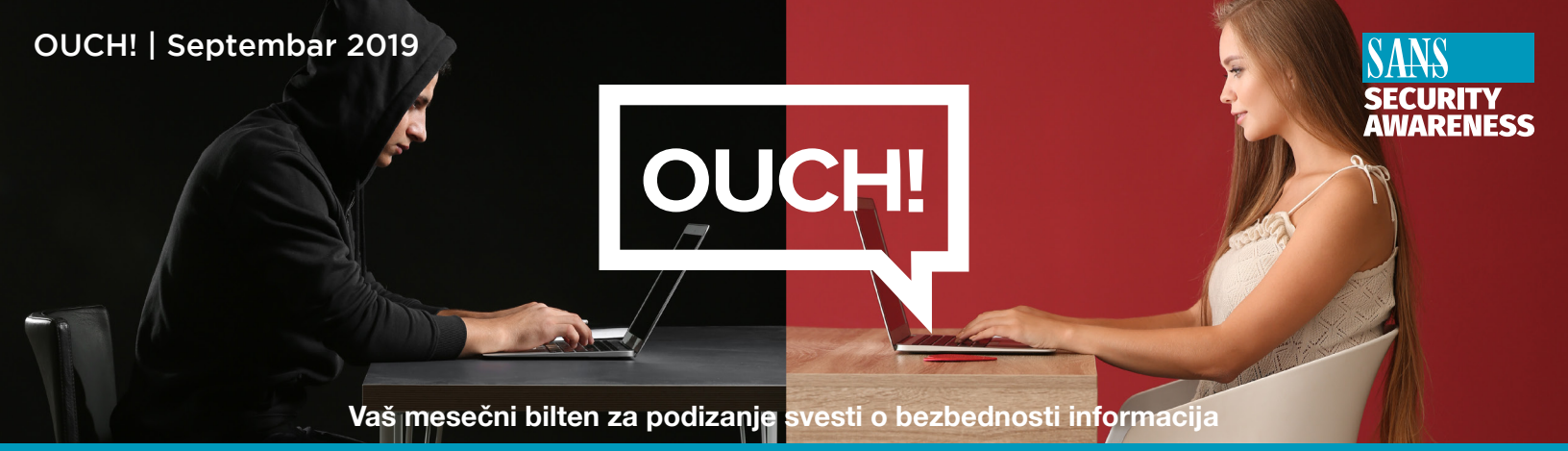
OUCH! | Septembar 2019



Vaš mesečni bilten za podizanje svesti o bezbednosti informacija

Prevare putem društvenih mreža

Uvod

Većini nas se dogodilo da bilo na poslu ili kod kuće budemo meta fišing napada putem elektronske pošte. Reč je o mejlovima koji samo izgledaju legitimno, kao da ih je poslala vaša banka, vaš šef ili vaša omiljena internet prodavnica, a zapravo su u pitanju napadi, kojima sajber kriminalci pokušavaju da vas zbrzaju ili prevare da preduzmete akciju koja će vam naštetiti, poput otvaranja zaraženog priloga iz mejla, odavanja vaše lozinke ili obavljanja prenosa novca. Izazov se ogleda u tome da što smo efikasniji u otkrivanju i zaustavljanju ovakvih napada putem elektronske pošte, sajber kriminalci sve više isprobavaju druge načine da ljude kontaktiraju i prevare.

Pokušaji prevare se mogu dogoditi u bilo kojoj formi komunikacije koju koristite, počev od Skajpa, Vatsapa i Sleka do Tvitera, Fejsbuka, Snepčeta, Instagrama, pa čak i aplikacija za igranje igrica. Komunikacija putem ovih platformi ili kanala korisnicima izgleda neformalno i pouzdano, što je upravo razlog zašto ih napadači koriste da prevare svoje žrtve. Dodatno, uz današnje tehnologije, bilo kom napadaču bilo gde u svetu postalo je mnogo lakše da se pretvara da je bilo šta ili bilo ko. Važno je zapamtiti da bilo koja komunikacija u kojoj učestvujete ne mora zaista biti onakva kakvom se čini i da ljudi nisu uvek oni za koje se predstavljaju.

Ključni znaci

U nastavku su opisani najčešći znaci koji ukazuju da poruka koju ste upravo primili ili objava koju ste upravo pročitali može biti napad.

Hitnost: Stvara se osećaj hitnosti i zahteva momentalna akcija pre nego što se desi nešto loše, prete vam na primer gašenjem naloga ili odlaskom u zatvor. Napadač želi da vas požuri kako biste napravili grešku.

Pritisak: Stvara se pritisak da zaobiđete ili ignorišete pravila ili procedure na poslu.

Radoznalost: Pobuđuje se snažno osećanje radoznalosti ili vas obaveštavaju o događaju koji je previše dobar da bi bilo istinit. Budite sigurni da niste pobedili na lutriji.

Osetljivost: Zahteva se da odate veoma osetljive informacije, poput broja kreditne kartice, lozinke ili bilo koje druge informacije koju jednostavno ne smete da delite.

Službene poruke: U poruci piše da dolazi od zvanične organizacije, ali poruka ima gramatičke ili pravopisne greške. Većina državnih institucija neće koristiti društvene mreže za zvaničnu komunikaciju direktno sa vama. Ako niste sigurni da je poruka legitimna, nazovite organizaciju, ali koristite pouzdan telefonski broj, poput onog sa njihove veb stranice.

Lažno predstavljanje: Dobili ste poruku od vašeg prijatelja ili kolege, ali ton ili izbor reči jednostavno ne deluju kao da vam se on obratio. Ukoliko sumnjate, pozovite pošiljaoca telefonom da proverite da li je zaista on poslao poruku. Sajber napadaču je lako da kreira poruke koje izgledaju kao da potiču od nekoga koga poznajete. U nekim slučajevima napadač može preuzeti nalog vašeg prijatelja, a zatim se pretvarati i obratiti vam se kao da je vaš prijatelj. Budite posebno oprezni kada su u pitanju tekstualne poruke, poruke koje se šalju preko Tvitera ili drugih platformi za slanje kratkih poruka, kod kojih je mnogo teže spoznati ko vam se zapravo obraća.

Vi sami ste najbolja odbrana od ovakvih prevara i napada. Kada poruka ili objava na društvenoj mreži deluje čudno ili sumnjivo jednostavno je ignorišite ili obrišite. U slučaju da takvu poruku primite od osobe koju lično poznajete, pozovite tu osobu telefonom da potvrdite da ju je zaista ona poslala.

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

Dr Džesika Barker *(@drjessicabarker) je ekspert za ljudsku stranu sajber bezbednosti. Ona je jedan od direktora u kompaniji Cygenta, u kojoj sledi svoju strast da u domenu sajber bezbednosti pozitivno utiče na promenu svesti, ponašanja i kulture širom sveta. Ona je predsedavajući foruma ClubCISO i popularni predavač na konferencijama.*

Dodatni materijal

Socijalni inženjering:	https://www.sans.org/u/Uz6
Telefonski napadi i prevare:	https://www.sans.org/u/Uzb
Ne dajte se upecati:	https://www.sans.org/u/Uzg
Personalizovane prevare:	https://www.sans.org/u/Uzl