Vaš mesečni bilten za podizanje svesti o bezbednosti informacija

# Emocionalni okidači - kako vas sajber kriminalci varaju

## Uvod

Sajber kriminalci neprestano smišljaju nove načine da nas prevare i navedu na akciju koju ne bismo trebali da preduzmemo, poput klika na maliciozni link, otvaranja zaraženog priloga elektronske pošte, kupovine lažne poklon kartice ili odavanja naše lozinke. Pored toga, oni za prevaru koriste različite tehnologije ili platforme, kao što su elektronska pošta, telefonski pozivi, tekstualne poruke ili društvene mreže. Iako sve ovo može izgledati veoma složeno, većina ovih napada oslanja se na isto, a to su vaše emocije. Poznavanje emocionalnih okidača koje sajber kriminalci koriste vam često može pomoći da prepoznate njihove napade bez obzira na tehnologiju ili platformu kojom se služe.

## Sve je u vezi sa emocijama

Sve počinje sa osećanjima. Mi, kao ljudi, prečesto donosimo odluke zasnovane na osećanjima umesto na činjenicama. U stvari, postoji čitava oblast proučavanja ovog koncepta koja se zove ekonomija ponašanja (eng. *behavioral economics*), kojom se bave istraživači Danijel Kaneman, Ričard Taler i Kas Sanstajn. Srećom, ako poznajemo emocionalne okidače od interesa, možemo uspešno uočiti i zaustaviti većinu napada. U nastavku teksta nevedeni su najčešći emocionalni okidači koji se koriste u sajber napadima. Sajber kriminalci neretko u istoj poruci elektronske pošte, tekstualnoj poruci, objavi na društvenim mrežama ili telefonskom pozivu koriste kombinaciju navedenih emocionalnih okidača, čime se povećava efikasnost napada.

**Hitnost**: Pojačan osećaj hitnosti je jedan od najčešćih emocionalnih okidača, upravo zbog svoje efikasnosti. Sajber kriminalci često koriste strah, anksioznost, oskudicu ili zastrašivanje da bi vas požurili da napravite grešku. Uzmite, na primer, da vam je stigla hitna elektronska poruka od vašeg šefa u kojoj vam traži da mu odmah pošaljete osetljiva dokumenta, dok se zapravo radi o sajber napadaču koji se pretvara da je vaš šef. Ili pretpostavimo da ste dobili tekstualnu poruku od sajber napadača koji se pretvara da je organ državne uprave koji vas obaveštava da kasnite sa uplatom poreza i da morate odmah da izvršite plaćanje kako ne biste završili u zatvoru.

**Ljutnja**: Može se javiti kada dobijete poruku o političkom, ekološkom ili društvenom pitanju do kog vam je veoma stalo – nešto poput „nećete verovati šta ova politička grupa ili korporacija radi!“

**Iznenađenje** / **Radoznalost**: Najuspešniji napadi su ponekad zasnovani na što manje informacija. Radoznalost se efikasno pobuđuje iznenađenjem, odnosno neočekivanom porukom. Želja da saznamo više je prirodan odgovor na nešto neočekivano. Na primer, sajber napadač vam je poslao poruku da paket nije isporučen i da treba da kliknete na link da biste saznali detalje, iako zapravo niste ništa naručili putem interneta. Na taj način zapravo bivamo namamljeni da kliknemo! Paketa naravno nema, a sa druge strane linka nas umesto njega čeka samo maliciozna namera.

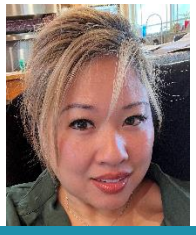
**Poverenje**: Kriminalci često koriste ime ili brend kome verujete da bi vas ubedili da preduzmete akciju. Na primer, takva je poruka u kojoj se pošiljalac pretvara da je iz vaše banke, poznate humanitarne organizacije, državne institucije od poverenja ili čak osobe koju poznajete. Budite na oprezu, to što se u mejl ili tekstualnoj poruci koristi ime i logo organizacije koju poznajete, ne znači i da poruka potiče od nje.

**Uzbuđenje**: Dobili ste, na primer, tekstualnu poruku od banke ili pružaoca usluga u kojoj vam se zahvaljuju što redovno plaćate njihove usluge. Tekstualna poruka sadrži link na kojem, nakon što kliknete, možete zatražiti nagradu – novi iPad, fenomenalno! Link vas vodi na veb sajt koji izgleda zvanično, ali od vas zahteva da unesete sve vaše lične podatke ili kompletne podatke o platnoj kartici da biste pokrili male troškove isporuke. U ovom slučaju se zapravo radi o sajber napadaču koji pokušava da ukrade vaš identitet ili novac.

**Empatija / Saosećanje**: Sajber napadači se ne ustručavaju da iskoriste vašu dobru volju. Na primer, nakon što se u medijima pojavi vest o nekoj katastrofi, oni će pripremiti i poslati milione lažnih mejlova u kojima se pretvaraju da su dobrotvorna organizacija koja pomaže ugroženima i tražiti od vas da uplatite prilog.

Ako se postarate da dobro razumete ove emocionalne okidače, bićete mnogo bolje pripremljeni da uočite i zaustavite sajber napad, bez obzira na to koji mamac, tehnologija ili platforma se koriste.

## Gost urednik



Mej-Nop Noin je izvršni direktor i glavni konsultant u kompaniji "Secured IT Solutions". Poseduje 20 godina iskustva u unapređivanju i upravljanju sajber bezbednošću i programima upravljanja rizicima kako u vladinom tako i u privatnom sektoru. Svoje iskustvo prenosi i kao sertifikovani instruktor SANS instituta, predajući na obuci MGT512. https://www.linkedin.com/in/menop, My-Ngoc Nguyen | SANS Institute @MenopN.

## Dodatni materijal

**Socijalni inženjering:** https://www.sans.org/newsletters/ouch/social-engineering-attacks/
**Telefonski napadi i prevare (višing):** https://www.sans.org/newsletters/ouch/vishing/
**Tri najčešće prevare na društvenim mrežama:** https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
**Napadi putem tekstualnih poruka - prepoznajte ih i sprečite:** https://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
**Čuvajte se, fišing napadi postaju sve napredniji:** https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/

Preveli za zajednicu: Dragan Ristić i Gordana Živanović