Vaš mesečni bilten za podizanje svesti o bezbednosti informacija

Tri najčešće prevare na društvenim mrežama

Uvod

Društvene mreže predstavljaju fantastičan način za komunikaciju, razmenu i zabavu sa drugima, ali su one u isto vreme i veoma jeftin alat koji sajber kriminalci mogu iskoristiti da prevare i iskoriste milione ljudi. U nastavku teksta saznajte kako da ne postanete žrtva tri najčešće prevare na društvenim mrežama.

Investicione prevare

Da li ste nekada videli objavu na društvenim mrežama o prilici za investiciju koja obećava ogroman povraćaj ulaganja u vrlo kratkom periodu, i to navodno bez rizika ili uz vrlo mali rizik? Ovde se zapravo radi o investicionim prevarama. Prevaranti će ukrasti vaš novac čim ga uplatite. Ovakve prevare često sadrže reklame ili svedočenja bivših klijenata o uspešnosti ulaganja kako bi se investicija dodatno promovisala, ali treba da znate da su to zapravo lažna svedočenja osmišljena sa ciljem da se poveća vaše poverenje. Neretko se ovakve prevare odnose na ulaganje u kriptovalute ili nekretnine, a plaćanje vrši u kriptovalutama ili drugim nestandardnim metodama plaćanja. Ako vam investicija deluje previše unosnom da bi bila moguća, najverovatnije je reč o prevari. Ne zaboravite, zagarantovane investicije sa visokom zaradom jednostavno ne postoje. Svoj novac investirajte samo na pouzdane, dobro poznate načine, a nikako kod stranaca koje ste upoznali na internetu i koji vam obećavaju brzo bogaćenje.

Romantične prevare

Kada kriminalci putem interneta stupe vezu sa nekim za koga su uočili da je usamljen ili ranjiv i to sa ciljem da od njega izvuku novac, reč je o prevari zasnovanoj na ljubavnim osećanjima, tzv. romantičnoj prevari. Kriminalaci koriste različite taktike za sticanje poverenja, uključujući i razmenu lažnih fotografija ili slanje poklona, nakon čega najčešće iznesu neku tužnu priču o tome kako im je potreban novac za plaćanje bolničkih računa ili putnih troškova. Da bi izbegli susret uživo, ovi kriminalci će verovatno tvrditi da se navodno bave poslom koji ih u tome sprečava, kao što je građevinarstvo, pružanje medicinskih usluga u inostranstvu ili služba u vojsci. Kako bi anonimno došli do novca, predložiće žrtvi da upotrebi transfer novca doznakom (eng. wire transfer) ili da im pošalje poklon kartice. Ovakve vrste prevara, pored društvenih mreža, česte su i u aplikacijama za upoznavanje na internetu. Budite na oprezu sa osobama koje upoznajete na internetu, ne brzajte već pažljivo promislite svaki korak i nikada ne šaljite novac nekome sa kim ste komunicirali samo putem interneta.

Dodatno, ako verujete da je neko koga poznajete možda ranjiv na ovakve napade ili znate da je u vezi na internetu koja budi sumnju, ponudite mu pomoć. Kada je neko zaokupljen snažnim osećanjima često mu je veoma teško da sam sagleda u kojoj meri je situacija postala opasna.

Prevare u kupovini putem interneta

Prevare u internet kupovini dešavaju se kada kupujete artikle na internetu po izuzetno niskim, neverovatnim cenama, koje na kraju nikada ne dobijete. Za ovu vrstu prevara koriste se primamljivi oglasi na društvenim mrežama u kojima se nude veoma niske cene i koji sadrže linkove do sajtova koji izgledaju kao da su legitimni i da prodaju proizvode poznatih brendova, a zapravo su lažni. Budite oprezni sa veb sajtovima na kojima nisu navedene kontakt informacije, kojima forme za kontakt ne funkcionišu, ili na kojima se kao kontakt podaci navode lične adrese elektronske pošte. Unesite ime internet prodavnice ili njenu veb adresu u pretraživač da biste videli šta su drugi kupci pisali o njoj. Potražite pojmove kao što su "prevara", "nikad više" ili "lažni" (eng. „fraud", „scam", „never again", „fake"). Pazite se internet promocija ili ponuda koje izgledaju previše dobro da bi bile istinite. Daleko je bezbednije kupiti predmete koji su malo skuplji, ali sa pouzdanih sajtova koje ste vi ili vaši prijatelji ranije koristili.

Znajte da ste vi sami vaša najbolja odbrana. Kontrola je u vašim rukama. Potrebno je samo da budete svesni opisanih prevara, da budete uvek na oprezu i moći ćete na bezbedan način da koristite društvene mreže u punom potencijalu.

Gost urednik

Kris Elgi (@chriselgee) je penetracioni tester i dizajner izazova za @CounterHackSec nadmetanja, komandant sajber bataljona američkih oružanih snaga i sertifikovani SANS instruktor. Uživa u proučavanju tehničkih detalja i njihovom ugrađivanju u suštinsko organizaciono razumevanje koje deli studentima i klijentima.

Dodatni materijal

Better Business Bureau Scam Tracker (SAD, Kanada, Meksiko): https://www.bbb.org/ScamTracker
Socijalni inženjering: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Kupujte bezbedno preko interneta: https://www.sans.org/newsletters/ouch/shopping-online-securely-nov-21/
Telefonski napadi i prevare (višing): https://www.sans.org/newsletters/ouch/vishing

Preveli za zajednicu: Dragan Ristić i Gordana Živanović