Vaš mesečni bilten za podizanje svesti o bezbednosti informacija

Prevare sa humanitarnim akcijama

Sajber kriminalci znaju da je stvaranje pojačanog osećaja hitnosti jedan od najboljih načina da ljude navedu na grešku. Jedan od najlakših načina da se stvori lažni osećaj hitnosti je da se iskoristi neka aktuelna kriza. Zbog toga sajber kriminalci željno iščekuju krizne događaje, posebno one sa globalnim uticajem. U dešavanjima koja većina nas doživljava kao tragediju, kao što su početak rata, velike prirodne katastrofe poput vulkanskih eksplozija, širenje zaraznih bolesti poput COVID-19, sajber kriminalci vide odličnu priliku. Kada društvene mreže i mediji počnu da se u velikoj meri bave nekim takvim događajima, sajber kriminalci znaju da je došlo vreme za sajber napad.

Sajber kriminalci koriste krizu tako što osmišljavaju fišing elektronske poruke i druge načine prevare koji se pozivaju na krizni događaj, a zatim u pravom trenutku pokreću takve napade nad milionima ljudi širom sveta. Na primer, tokom prirodne katastrofe, oni se mogu pretvarati da su humanitarna organizacija koja traži donacije za spas dece u nevolji. Sajber kriminalci se pripremaju unapred, imaju spremnu svu tehničku infrastrukturu, zbog čega su vrlo često u stanju da deluju u roku od samo nekoliko sati nakon krize ili katastrofe. Kako da se zaštitimo od sajber kriminalaca koji žele da iskoriste krizu ili katastrofu?

Kako prepoznati ove napade i kako da se od njih odbranite

Ključ za izbegavanje ovih prevara je da budete sumnjičavi prema svakom ko vam se obrati. Na primer, nemojte verovati hitnoj mejl poruci koja izgleda kao da je šalje humanitarna organizacija kojoj hitno trebaju donacije, čak i ako mejl izgleda kao da ga je poslala organizacija koju poznajete i kojoj verujete. Ne verujte telefonskom pozivu u kojem pozivalac tvrdi da zove ispred lokalne narodne kuhinje i ubeđuje vas da donirate. Što je veći pritisak ili osećaj hitnosti, veća je verovatnoća da je u pitanju napad. U nastavku teksta navedeni su najčešći znaci ovakvih prevara:

- Budite veoma sumnjičavi prema humanitarnim organizacijama koje vam traže da donirate putem kriptovaluta, Western Union-a, elektronskog transfera novca ili poklon kartica.
- Znajte da sajber kriminalci mogu da promene broj telefona koji se vama prikazuje kao identifikacija pozivaoca kako bi njihov telefonski poziv izgledao kao da je lokalni ili da ga upućuje neko kome verujete. Zato vam savetujemo da ne verujete identifikaciji pozivaoca.
- Neki sajber kriminalci mogu da korise imena i logoe koji zvuče ili izgledaju kao da pripadaju pravoj dobrotvornoj organizaciji. Pre nego što donirate, obavezno proverite da li se zaista radi o pravoj organizaciji.
- Sajber kriminalci često iznose različite nejasne i emotivne tvrdnje o tome šta će sve uraditi sa vašim novcem, ali ne navode nikakve detalje o tome kako će se vaša donacija zaista koristiti.
- Budite sumnjičavi prema molbama za pomoć na sajtovima za prikupljanje sredstava kao što je GoFundMe ili na društvenim mrežama kao što je TikTok, posebno nakon neke krize ili tragedije.

- Neki sajber kriminalci mogu pokušati da vas prevare i navedu da donirate novac tako što će vam se zahvaliti na donaciji koju ste im dali u prošlosti, iako im vi zapravo nikada niste uputili donaciju.
- Kada odgovarate na zahtev koji vam je stigao neočekivano, nikada ne odajte lične ili finansijske podatke.

Kako da pomognete na bezbedan način

Da biste donirali u kriznim vremenima i pomogli onima koji su pogođeni katastrofom, donirajte samo dobro poznatim organizacijama od poverenja. Nastojte da vi budete strana koja inicira komunikaciju i da sami odlučujete kome ćete se obratiti, na primer koje veb sajtove ćete posetiti ili koje organizacije ćete pozvati. Dok razmatrate da li da donirate određenoj humanitarnoj organizaciji, pokrenite pretragu koristeći naziv te organizacije i reči kao što su žalba, pregled, ocena ili prevara (ili engleski: compliant, review, rating, scam). Niste sigurni kojim humanitarnim organizacijama da verujete? Započnite istraživanje na veb sajtovima državnih organa kojima verujete, ili na zvaničnim sajtovima poznatih medijskih organizacija kojima se veruje. Doniranje u kriznim vremenima je odličan način da pomognete, samo se prethodno uverite da se radi o legitimnim organizacijama.

Gost urednik

Dr. Džesika Bejker je nagrađivana liderka koja se bavi ljudskom stranom sajber bezbednosti. Jedna je od izvršnih direktora u kompaniji Cygenta i autorka je bestselera. Članica je savetodavnog odbora SANS-ovog samita o podizanju svesti o bezbednosti informacija.

Dodatni materijal

FTC Charity Fraud: https://consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams
Socijalni inženjering: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
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/
Telefonski napadi i prevare (višing): https://www.sans.org/newsletters/ouch/vishing/
Charity Navigator: https://www.charitynavigator.org/

Preveli za zajednicu: Dragan Ristić i Gordana Živanović