Krāpnieki krīzes situācijās

Kibernoziedznieki zina, ka viens no labākajiem veidiem, kā pamudināt cilvēkus pieļaut kļūdu, ir radīt steidzamības izjūtu. Viens no vienkāršākajiem veidiem, kā radīt steidzamības izjūtu, ir izmantot krīzes situāciju. Tāpēc kibernoziedznieki ir apmierināti, kad notiek kāds traģisks notikums ar globālu ietekmi. To, ko lielākā daļa no mums uzskata par traģēdiju, kibernoziedznieki uzskata par iespēju, piemēram, kara izcelšanos, lielu dabas katastrofu, kā vulkāna eksploziju, un, protams, tādu infekcijas slimību izplatību kā Covid-19. Ja pastāv milzīgs skaits sociālo mediju publikāciju un ziņu par noteiktu notikumu, kibernoziedznieki zina, ka ir pienācis laiks sākt uzbrukumu.

Viņi izmanto šo iespēju, lai savlaicīgi izveidotu pikšķerēšanas e-pasta vēstules vai krāpnieciskus ziņojumus par šo notikumu un pēc tam tās nosūtītu vai uzsāktu krāpšanu, kas vērsta pret miljoniem cilvēku visā pasaulē. Piemēram, dabas katastrofas laikā viņi var izlikties par labdarības organizāciju un lūgt ziedojumus, lai glābtu grūtībās nonākušos bērnus. Kibernoziedznieki bieži vien mēdz rīkoties dažu stundu laikā pēc krīzes vai katastrofas, jo viņiem ir sagatavota visa tehniskā infrastruktūra un viņi ir gatavi jau iepriekš. Kā mēs varam sevi pasargāt nākamreiz, kad notiks liela krīze vai katastrofa un kibernoziedznieki centīsies to izmantot?

Kā atpazīt un aizsargāties pret šādiem krāpšanas gadījumiem

Galvenais nosacījums, lai izvairītos no šiem krāpšanas gadījumiem, ir būt aizdomīgam pret ikvienu, kas jūs uzrunā. Neuzticieties e-pasta ziņojumam, kas jūs steidzina un kuros apgalvots, ka tos sūta labdarības organizācijas, kurām steidzami nepieciešami ziedojumi, pat ja šis e-pasts ir no zīmola, kuru pazīstat un kuram uzticaties. Neuzticieties tālruņa zvanam, kas uzdodas par vietējās pārtikas izsniegšanas labdarības pārstāvjiem un piespiež jūs ziedot. Jo lielāka steidzamības izjūta, jo lielāka iespēja, ka lūgums ir uzbrukums. Šeit ir minētas dažas visbiežāk sastopamās labdarības krāpšanas pazīmes:

- Esiet piesardzīgs ar labdarības organizācijām, kas pieprasa ziedot, izmantojot kriptovalūtu, Western Union, naudas pārskaitījumus vai dāvanu kartes.
- Kibernoziedznieki var mainīt zvanītāja tālruņa numuru, lai zvans izskatītos kā veikts no jūsu vietējās teritorijas koda vai uzticama zvanītāja. Mūsdienās nevar paļauties uz zvanītāja identitāti.
- Daži kibernoziedznieki izmanto nosaukumus un logotipus, kas izklausās vai izskatās kā īstas labdarības organizācijas. Tas ir viens no iemesliem, kāpēc pirms ziedošanas ir vērts padomāt.
- Kibernoziedznieki bieži vien izsaka daudz neskaidru un sentimentālu apgalvojumu par to, ko viņi darīs ar jūsu naudu, bet nesniedz nekādu konkrētu informāciju par to, kā jūsu ziedojums tiks izmantots.
- Neuzskatiet, ka lūgumi pēc palīdzības pūļa finansējuma vietnēs, piemēram, GoFundMe, vai sociālajos tīklos, piemēram, TikTok, ir likumīgi, jo īpaši pēc krīzes vai traģēdijas.

- Daži kibernoziedznieki var mēģināt jūs pierunāt ziedot viņiem, sakot paldies par agrāk veikto ziedojumu, lai gan patiesībā jūs viņiem nekad neesat ziedojis.
- Nesniedziet personisku vai finansiālu informāciju, atbildot uz nevēlamiem pieprasījumiem.

Kā palīdzēt droši

Lai ziedotu vai lai palīdzētu katastrofas skartajiem, ziedojiet tikai labi zināmām un uzticamām organizācijām. Jūs uzsākat kontaktu un izlemjat, ar ko sazināties, piemēram, kādas vietnes apmeklēt vai kādām organizācijām zvanīt. Kad apsverat iespēju ziedot kādai labdarības organizācijai, meklējiet tās nosaukumu un tādus vārdus kā "sūdzība", "atsauksme", "vērtējums" vai "krāpšana". Neesat pārliecināts, kurām labdarības organizācijām uzticēties? Sāciet ar izpēti valdības tīmekļa vietnēs, kurām uzticaties, vai ar saitēm, ko nodrošina kāda labi zināma un uzticama ziņu organizācija. Ziedošana grūtos brīžos ir lielisks veids, kā palīdzēt, taču pārliecinieties, ka ziedojat likumīgām organizācijām.

Viesredaktors

Dr. Džesika Bārkere (Jessica Barker) ir godalgota eksperte drošības jomās, kas saistītas ar cilvēku uzvedību. Viņa ir Cygenta līdzpriekšsēdētāja un populāru grāmatu autore. Džesika ir SANS Security Awareness Summit konsultatīvās padomes locekle.

Resursi

FTC labdarību krāpšana: https://consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams
Sociālā inženierija: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Trīs populārākie krāpniecības veidi: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Krāpšana ziņojumapmaiņā: https://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
Zvanu krāpniecība: https://www.sans.org/newsletters/ouch/vishing/
Labdarības navigators: https://www.charitynavigator.org/

Tulkojums: CERT.LV