

OUCH!

Ikmēnēša informācijas drošības izdevums tev

Trīs populārākie krāpšanas veidi sociālajos tīklos

Pārskats

Lai gan sociālie tīkli ir lielisks veids, kā sazināties, dalīties un izklaidēties ar citiem, tas ir arī lēts veids, kā kibernoiedznieki var maldināt un izmantot miljoniem cilvēku. Nekļūstiet par upuri trim izplatītākajām krāpšanas metodēm sociālajos tīklos.

Investīciju krāpniecība

Vai esat kādreiz redzējuši ziņu par ieguldījumu iespēju, kas sola milzīgu peļņu no ieguldījumiem ļoti īsā laikā, turklāt ar it kā nelielu risku vai bez tā? Realitāte ir tāda, ka šīs garantijas patiesībā ir ieguldījumu izkrāpšana. Krāpnieki vienkārši nozog jūsu naudu, kad esat viņiem samaksājis. Šīs krāpniecības bieži ietver reklāmas vai iepriekšējo klientu veiksmes stāstus, lai veicinātu ieguldījumus, taču tās ir tikai viltotas atsauksmes, lai palielinātu jūsu uzticību. Bieži vien investīciju krāpniecības ir saistītas ar investīcijām kriptovalūtās vai nekustamajā īpašumā, un maksājumi bieži tiek veikti kriptovalūtās vai izmantojot citas nestandarta maksāšanas metodes. Ja ieguldījumu iespēja šķiet pārāk laba, lai būtu patiesība, visticamāk, tā arī ir. Atcerieties, ka nepastāv garantēti augstas peļņas ieguldījumi. Ieguldiet naudu tikai uzticamos, zināmos resursos, nevis internetā sastaptos svešiniekos, kas piedāvā ātras peļņas shēmas.

Romantiskā izkrāpšana

Ja noziedznieks veido attiecības tiešsaistē ar kādu personu, kura ir identificēta kā vientuļa vai neaizsargāta, lai izvilienātu no tās naudu, tā tiek dēvēta par romantisko krāpšanu. Noziedznieks izmantos visas iespējamās taktikas, lai radītu uzticību, tostarp apmainīsies ar viltotām fotogrāfijām vai nosūtīs dāvanas, un pēc tam pastāstīs traģisku stāstu par naudas nepieciešamību, lai segtu izdevumus, piemēram, slimnīcas rēķinus vai ceļa izdevumus upura apmeklējumam klātienē. Lai izvairītos no tikšanās klātienē, šie noziedznieki var teikt, ka strādā nozarē, kas viņiem liedz to darīt, piemēram, celtniecībā, starptautiskajā medicīnā vai militārajā jomā. Viņi bieži pieprasa naudu kā pārskaitījumu vai dāvanu karti, lai ātri saņemtu naudu un paliktu anonīmi. Šāda veida krāpniecība ir izplatīta ne tikai sociālajos tīklos, bet arī tiešsaistes iepazīšanās lietotnēs. Esiet piesardzīgi ar cilvēkiem, kurus satiekat tiešsaistē, rīkojieties apdomīgi un nekad nesūtiet naudu personai, ar kuru esat sazināties tikai tiešsaistē.

Turklāt, ja uzskatāt, ka kāds jums pazīstams cilvēks var būt neaizsargāts pret šādu uzbrukumu vai veido attiecības tiešsaistē, kam raksturīgas šīs krāpšanas pazīmes, piedāvājiēt viņam palīdzību. Dažkārt kādam, kas ir iegrimis emocionālā saiknē, var būt ļoti grūti saprast, cik bīstama ir situācija.

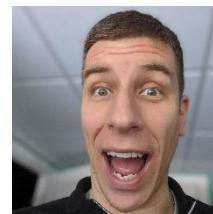
Tiešsaistes iepirkšanās krāpniecība

Tiešsaistes iepirkšanās krāpniecība notiek, kad iegādājaties preces tiešsaistē par ārkārtīgi zemām vai neticamām cenām, bet nesaņemat pirkumu. Kārdinošas reklāmas sociālajos tīklos mēdz reklamēt neticamas cenas, un tajās būs saites, kas novirzīs uz vietnēm, kas šķiet likumīgas un pārdod labi pazīstamus zīmolus, taču šīs vietnes bieži ir viltotas. Esiet piesardzīgi ar vietnēm, kurās nav kontaktinformācijas, saziņas veidlapa nedarbojas vai kurās tiek izmantotas personīgās e-pasta adreses. Ievadiet tiešsaistes veikala nosaukumu vai tā tīmekļa adresi meklētājprogrammā, lai redzētu, ko citi par to ir teikuši. Meklējiet tādus terminus kā “krāpšana”, “vairs nekad” un “viltota”. Esiet ļoti piesardzīgs ar tiešsaistes akcijām vai piedāvājumiem, kas šķiet pārāk labi, lai būtu patiesība. Daudz drošāk ir iegādāties preces, kas var maksāt nedaudz vairāk, bet no uzticamām vietnēm, kuras jūs vai jūsu draugi jau esat izmantojuši.

Labās ziņas ir šādas: Jūs esat sava labākā aizsardzība. Jūs kontrolējat situāciju. Esiet uzmanīgs pret šādiem krāpniecības centieniem, un jūs varēsiet droši izmantot sociālo tīklu iespējas.

Viesredaktors

Kriss Eldžijs (Chris Elgee) (@chriselgee) ir @CounterHackSec ielaušanās testētājs un uzdevumu izstrādātājs, armijas Nacionālās gvardes kiberbataljona komandieris un sertificēts SANS instruktors. Viņam patīk apgūt sarežģītas tehniskas nianšes, veidot no tām plašāku izpratni, un dalīties tajā ar studentiem un klientiem..



Resursi

“Better Business Bureau” krāpšanas izsekotājs: <https://www.bbb.org/ScamTracker>

Sociālā inženierija: <https://www.sans.org/newsletters/ouch/social-engineering-attacks/>

Droša iepirkšanās tiešsaistē: <https://www.sans.org/newsletters/ouch/shopping-online-securely-nov-21/>

Tālrūņa zvanu uzbrukumi un krāpniecība: <https://www.sans.org/newsletters/ouch/vishing/>

Tulkojums: CERT.LV

OUCH! To publicējis “SANS Security Awareness”, un tas tiek izplatīts saskaņā ar [“Creative Commons BY-NC-ND” 4.0 licenci](https://creativecommons.org/licenses/by-nc-nd/4.0/). Jūs varat brīvi koplietot vai izplatīt šo rakstu, kamēr vien jūs to nepārdodat un nepārveidojat. Redakcijas kolēģija: Valters Skrivenss (Walter Scrivens), Fils Hofmans (Phil Hoffman), Alans Vagoners (Alan Waggoner), Leslija Ridauta (Leslie Ridout), Princesa Janga (Princess Young).