OUCH! 2025. gada augusts

Jūsu ikmēneša informatīvais biļetens drošības izpratnes veicināšanai

Krāpniecības atpazīšana, meklējot darbu internetā

Marijas “sapņu darbs”, kas pārvērtās murgā

Marija tikko bija pabeigusi koledžas studijas un ļoti vēlējās iegūt savu pirmo pilnas slodzes attālināto darbu. Tāpēc, kad viņa saņēma ziņu LinkedIn platformā no kāda cilvēka, kurš apgalvoja, ka ir personāla atlases speciālists globālā tehnoloģiju uzņēmumā, viņa bija sajūsmā. Darba piedāvājums bija “attālinātais administratīvā asistenta darbs” – alga 4000 ASV dolāru mēnesī, elastīgs darba laiks un viss aprīkojums nodrošināts. Pēc viņas profila izvērtēšanas, personāla atlases speciālists vēlējās nekavējoties uzaicināt viņu uz darba pārrunām.

Intervija notika nākamajā dienā, izmantojot ziņapmaiņas lietotni. Bija mazliet dīvaini, bet personāla atlases speciālists paskaidroja, ka uzņēmums pilnībā pāriet uz attālinātu darbu. Pēc īsas 20 minūšu sarunas Marijai tika paziņots, ka viņa ir pieņemta darbā. Tad sekoja nākamie soļi: viņai bija jāaizpilda darbā iekārtošanās dokumenti, tostarp jānorāda savs personas kods, bankas informācija, autovadītāja apliecība un jāiesniedz sava fotogrāfija personāla uzskaitei.

Pēc dažām dienām viņa saņēma čeku 5000 ASV dolāru apmērā, lai iegādātos klēpjdatoru un programmatūras. Viņai tika uzdots iemaksāt šo čeku un pēc tam ar bankas pārskaitījumu nosūtīt 3800 ASV dolārus “apstiprinātajam” klēpjdatora piegādātājam, bet atlikušo naudu paturēt papildu izdevumiem.

Marija izpildīja norādījumus, bet pēc trim dienām ar viņu sazinājās banka. Čeks izrādījās viltots. Marija ne tikai zaudēja naudu, bet arī izpauda ļoti sensitīvu informāciju par sevi, kas, visticamāk, tiks izmantota identitātes zādzībai. Viņas sajūsma par jaunu karjeras iespēju bija aizēnojusi brīdinājuma zīmes.

Kā tiek īstenoti krāpnieciski darba piedāvājumi?

Krāpnieciski darba piedāvājumi darbojas gana efektīvi, jo tiek izmantos jūsu emocijas un steidzamības faktors. Ja esat bez darba, izjūtat spiedienu vai vienkārši esat sajūsmināts par šķietami labu iespēju, ir viegli nepamanīt brīdinājuma signālus. Krāpnieki sūta arī e-pasta vēstules, kas izskatās profesionālas, izmanto reālu uzņēmumu mājas lapu adreses un pat viltotus tālruņa numurus, lai izskatītos pēc "īsta" uzņēmuma. Nereti krpāšana sākas ar pārliecinošu sludinājumu ievietošanu sociālajos tīklos, bieži vien par attālinātu darbu vai elastīgu darba laiku. Pēc tam viņi sazinās ar jums e-pastā vai, iespējams, raksta Facebook ziņu, piedāvājot darbu. Lai iegūtu jūsu uzticību, krāpnieki bieži izliekas par reālu uzņēmumu pārstāvjiem. Pēc savstarpējas saziņas krāpnieki, izmantojot e-pastu, īsziņas vai tērzēšanas lietotnes, lai veiktu viltus darba interviju. Drīz pēc tam seko “darba piedāvājums”.

Viņu galvenais mērķis ir iegūt jūsu naudu,vai kā Marijas gadījumā, vai iegūt sensitīvu informāciju, lai varētu nozagt jūsu identitāti un veikt krāpšanu jūsu vārdā.

Brīdinājuma zīmes, kam pievērst uzmanību

Lai gan šie krāpšanas veidi kļūst aizvien izsmalcinātāki, ir daži "sarkanie karogi", kuriem varat pievērst uzmanību.

- **Pārāk labi, lai būtu patiesība**: Ļoti augsts atalgojums par mazu darba apjomu, tūlītēji darba piedāvājumi bez intervijas, darba piedāvājumi, kas nepārprotami pārsniedz jūsu kvalifikāciju, vai solījumi ātri pieņemt jūs darbā.
- **Spiediens rīkoties ātri**: krāpnieki vēlas, lai jūs uzņematies saistības, pirms jums ir laiks padomāt vai veikt izpēti.
- **Vispārīgi darba apraksti**: ja darba sludinājums ir neskaidrs vai pārāk vispārīgs, esiet piesardzīgs. Uzticami darba devēji parasti norāda detalizētu amata aprakstu un prasīto kvalifikāciju.
- **Maksājumu pieprasījumi**: jums nekad nevajadzētu maksāt par apmācībām, iepriekšēju pārbaudi saistībā ar darbu vai segt darba aprīkojuma izmaksas.
- **Dīvaina saziņa**: ar aizdomām izturieties pret darba piedāvājumiem, ja saņemat tos no Gmail, Yahoo vai līdzīgām privātā e-pasta adresēm. Īsti personāla atlases speciālisti parasti izmanto korporatīvos e-pasta kontus. Pievērsiet uzmanību, vai netiek pārmērīgi izmantotas ziņapmaiņas lietotnes un izvairieties no tālruņa vai video zvaniem. Vienmēr esiet īpaši piesardzīgs attiecībā uz saziņu, kuru jūs neesat ierosinājis.
- **Slēpta uzņēmuma informācija**: ja uzņēmumu nevarat atrast tiešsaistē vai tam nav sava mājas lapa, LinkedIn/ Facebook profils vai kaut kas izskatās aizdomīgi, rīkojieties piesardzīgi.

Kā sevi pasargāt

Jūs varat izmantot tiešsaistes darba iespējas, vienlaikus ievērojot drošības pamatprincipus – tikai veiciet dažus piesardzības pasākumus:

- Vienmēr pārbaudiet darba devēju, veiciet izpēti, un apmeklējiet uzņēmuma oficiālo mājas lapu un pārliecinieties, ka vakance ir publicēta.
- Izmantojiet uzticamas darba meklēšanas tīmekļa vietnes un profesionālos tīklus. Tajos ir mazāka viltus darba piedāvājumu iespējamība, taču pavisam izslēgt šādu varbūtību nevar.
- Sākotnējās sarunās nekad nesniedziet savus datus - personas kodu, bankas konta vai personu apliecinošu dokumentu kopijas.

Ja rodas sajūta, ka kaut kas nav kārtībā, visticamāk, tā arī ir. Mēģiniet paskaties uz situāciju no malas un aprunājies ar kādu uzticamu cilvēku. Jo lielāka steidzamības sajūta tiek radīta, jo lielāka iespējamība, ka tā ir krāpniecība.

Viesredaktore

Dona Ross (Donna Ross) ir uzņēmuma Radian izpildviceprezidente un galvenā informācijas drošības speciāliste. Viņai ir vairāk nekā 25 gadu pieredze kiberdrošības, un uzņēmumu risku pārvaldības jomā dažādās nozarēs, tostarp finanšu, veselības aprūpes, apdrošināšanas un ražošanas jomā, un viņa ir atbildīga par Radian informācijas drošības, risku mazināšanas un privātuma funkcijām, koncentrējoties uz stratēģiju, noturību un pārvaldību.

Resursi

Krāpnieciskas investīcijas, balstītas uz viltus romantiskām attiecībām: https://www.sans.org/newsletters/ouch/sweet-talk-empty-wallet-romance-fueled-investment-scams/
Krāpnieciskas investīcijas, balstītas uz viltus romantiskām attiecībām: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
Kontu pārņemšana: Emocionālie plēsēji: https://www.sans.org/newsletters/ouch/account-takeovers-emotional-predators/

CERT.LV