OUCH! 2025. gada maijs

OUCH!

SANS SECURITY AWARENESS

Jūsu ikmēneša informatīvais biļetens drošības izpratnes veicināšanai

Kā kibernoziedznieki izmanto jūsu emocijas?

Īsziņa ar augstu cenu

Emma bija izgājusi tik tikko no pārtikas veikala ar vairākiem maisiņiem rokās, kad viņas tālrunī pienāca īsziņa no meitas.

"Mammu, es pazaudēju savu telefonu! Es rakstu no drauga telefona. Man vajag naudu jaunam. Lūdzu, atsūti tagad 800 USD — es paskaidrošu vēlāk!"

Emmas sirds sastinga. Viņas meita Endžija atradās koledžā un Emma zināja, cik svarīgs telefons ir Endžijas mācībām, darbam un saziņai. Doma par to, ka viņa paliks bez telefona, Emmu satrauca. Viņa ātri atbildēja:

"Vai ar tevi viss kārtībā? Kas notika?"

Atbilde pienāca gandrīz nekavējoties.

"Man viss ir kārtībā, bet es nevaru tagad runāt. Es aizņēmos drauga telefonu. Vai vari man tagad atsūtīt naudu? Man vajadzīgs jauns telefons pēc iespējas ātrāk! Es tev šovakar piezvanīšu. Mīlu tevi!"

Emma brīdi vilcinājās. Kaut kas šķita nepareizi, taču viņas bažas izrādījās stiprākas par šaubām. Viņa atvēra bankas lietotni un pārskaitīja 800 USD uz īsziņā norādīto tālruņa numuru. Viņai pat neradās aizdomas, kādēļ nauda netiek pārskaitīta tieši meitas kontā — varbūt Endžija nevarēja tam piekļūt bez tālruņa.

Vēlāk vakarā viņa piezvanīja uz īsto Endžijas numuru, sagaidot, ka viņas balsī dzirdēs atvieglojumu. Taču viņa atbildēja kā parasti.

"Sveika, mamma! Kā iet?"

Emma sastinga.

"Vai tu saņēmi naudu?"

Endžija izklausījās apjukusi.

"Kādu naudu?"

Emmas sirds apmeta kūleni. Viņa atkal atvēra īsziņas, pārlasot tās ar svaigu skatu. Steidzīgais tonis, konkrētas informācijas trūkums, uzstājīgā prasība nekavējoties veikt maksājumu — tas viss pēkšņi norādīja uz **krāpšanu**. Krāpnieks izlikās par Emmas meitu, jo zināja, ka māte panikā nepārbaudīs situāciju.

Diemžēl Emmas pieredze nav unikāla. Kibernoziedznieki ik dienu manipulē ar emocijām, lai piespiestu cilvēkus pieļaut dārgi maksājošas kļūdas. Lūk, pieci biežāk sastopamie krāpnieku izmantotie emociju izraisītāji un kā tos pamanīt, pirms vēl nav par vēlu.

1. Steidzamība — “Rīkojies uzreiz vai kaut ko zaudēsi!”

Krāpnieki rada viltus steidzamības sajūtu, lai piespiestu jūs pieņemt sasteigtus lēmumus.

Kā tas notiek:

“Jūsu bankas konts ir uzlauzts! Divu stundu laikā apstipriniet savu identitāti, citādi jūsu līdzekļi tiks iesaldēti.”

- *“Jūsu maksājums ir pabeigts.” (kad zināt, ka neesat iegādājies preci)*
- *“Jūsu paroles derīguma termiņš tuvojas beigām! Atjauniniet to tagad, klikšķinot šeit.”*

Kā pamanīt krāpšanu:

- Sazinieties ar uzņēmumu tieši — izmantojiet oficiālo kontaktinformāciju, piemēram, zvaniet uz uzticamu tālruņa numuru vai izmantojiet uzņēmuma mobilo lietotni.
- Pārbaudiet, vai ziņojumā ir skaidra informācija — reāli uzņēmumi sniedz precīzu informāciju, nevis izsaka draudus.

2. Bailes — “Notiks kaut kas slikts!”

Kibernoziedznieki izmanto bailes, lai radītu paniku un piespiestu upurus rīkoties nedomājot.

Kā tas notiek:

- *“Mēs esam valsts iestāde. Jums ir izveidojies nodokļu parāds un tas jāsamaksā nekavējoties, citādi jūs arestēs!”*
- *“Jūsu ierīcē ir atklāts vīruss! Zvaniet uz šo numuru, lai saņemtu atbalstu.”*
- *“Ja nemaksāsiet šo izpirkuma maksu, jūsu privātie fotoattēli tiks nopludināti.”*

Kā pamanīt krāpšanu:

- Valsts iestādes nesūta draudus īsziņās vai e-pastā.
- Tehnoloģiju uzņēmumi nesazināsies ar jums, lai piedāvātu salabot jūsu datoru.

3. Ziņkārība — “Jūs nespēsiet tam noticēt!”

Krāpnieki izmanto cilvēku ziņkārību, nosūtot šokējošas vai vilinošas ziņas.

Kā tas notiek:

- *“Vai tu esi šajā video? 😳” (nosūtot kopā ar ļaunprātīgu saiti)*
- *“Šokējošas ziņas! Milzīgs skandāls, kurā iesaistītas slavenības — klikšķiniet šeit, lai redzētu.”*
- *“Tavs draugs atzīmēja tevi trakulīgā ierakstā!”*

Kā pamanīt krāpšanu:

- Izturieties skeptiski pret sensacionāliem ziņojumiem.
- Pirms klikšķināt uz jebkuras saites, sazinieties ar sūtītāju.

4. Uzticība un autoritāte — “Tas ir kāds, kuru jūs pazīstat!”

Kibernoziedznieki izliekas par uzticamiem cilvēkiem — priekšniekiem, bankām vai pat tuviniekiem.

Kā tas notiek:

- *"Sveiki, mammu, tas esmu es! Es pazaudēju savu telefonu! Vai vari atsūtīt naudu?"*
- *"Šeit jūsu priekšnieks Man ir nepieciešams, lai jūs iegādātos dāvanu kartes biroja pasākumam."*
- *"Jūsu kontā tika konstatētas aizdomīgas darbības. Klikšķiniet šeit, lai padarītu kontu drošu!"*

Kā pamanīt krāpšanu:

- Kopā ar ģimenes locekļiem izveidojiet slepenu paroli, kas ļautu pārbaudīt sūtītāja identitāti.
- Pievērsiet uzmanību vispārīgiem ziņojumiem — krāpnieki parasti nezina jūsu vārdu vai pasta adresi.
- Uzmanīgi izturieties pret neparastiem pieprasījumiem, jo īpaši tādiem, kas saistīti ar naudu vai sensitīvu informāciju.

5. Prieks un alkatība — "Jūs esat laimējis kaut ko lielisku!"

Krāpnieki rada situācijas, kas izklausās pārāk labi, lai būtu patiesas, izmantojot cilvēku vēlmi kaut ko iegūt vai saņemt uzmanību.

Kā tas notiek:

- *"Apsveicam! Jūs laimējāt bezmaksas iPhone — saņemiet to tūlīt!"*
- *"Man šķiet, ka tu esi brīnišķīgs cilvēks, pastāsti man par sevi vairāk."*
- *"Esmu izvēlējies tieši jūs dalībai ekskluzīvā investīciju iespējā!"*

Kā pamanīt krāpšanu:

- Ja nepiedalījāties loterijā, jūs noteikti nelaimējāt balvu. Īsti uzņēmumi neprasa maksāt naudu, lai saņemtu balvu.
- Uzmanīgi izturieties pret svešiniekiem, kuri uzstājīgi piedāvā kaut ko, kas izklausās "pārāk labi, lai būtu patiesība", vai kuri pārāk ātri pauž romantiskas jūtas.
- Esiet skeptiski noskaņoti pret "ekskluzīviem" piedāvājumiem, kas nosūtīti nejauši izvēlētiem cilvēkiem.

Nākamreiz, kad saņemsiet steidzamu īsziņu vai tālruņa zvanu, apstājieties, padomājiet un pārbaudiet, pirms rīkojaties. Neļaujiet emocijām kļūt par jūsu vājo vietu!

Viesredaktore

Terēza Gērke (Teressa Gehrke) ir uzņēmuma PopCykol, kas nodarbojas ar drošību un izpratni par drošību tiešsaistē, dibinātāja. Viņai ir vairāk nekā 10 gadu pieredze nozarē, strādājot par tehnisko tekstu autori, UX dizaineri un projektu vadītāju. Viņa ir WiCyS Colorado valdes locekle. Terēza ir godalgota mūziķe. Linktree

Resursi

Investīciju krāpniecība, izmantojot viltus romantiskus nodomus: https://www.sans.org/newsletters/ouch/sweet-talk-empty-wallet-romance-fueled-investment-scams/
Aizsardzība pret balss klonēšanas uzbrukumiem: https://www.sans.org/newsletters/ouch/phantom-voices-defend-against-voice-cloning-attacks/
Teksta ziņojumapmaiņas uzbrukumi: Smikšķerēšanas sāga: https://www.sans.org/newsletters/ouch/text-messaging-attacks-smishing-saga/

CERT.LV