OUCH! 2026. gada janvāris

OUCH!

Workforce Security and Risk Training

Ikmēneša informatīvais biļetens drošības izpratnes veicināšanai

Viltus tehniskais atbalsts: vienīgais, ko viņi "salabo", ir jūsu bankas konts

Kā "palīdzības" zvans pārvērtās par dārgu pieredzi

Aiša strādāja no mājām, kad pēkšņi uz viņas klēpjdatora parādījās pārlūka uznirstošais loga ***"Jūsu Windows operētājsistēma vairs netiek atbalstīta un, šķiet, ir inficēta! Jūsu personas dati, bankas informācija un cita sensitīvā informācija, visticamāk, ir apdraudēta. Drošības nolūkos, lūdzu, nekavējoties sazinieties ar Windows tehnisko atbalstu. Zvaniet tūlīt: 1 8XX XXX XXXX***

Uztraukusies, ka varētu zaudēt savus līdzekļus un datnes, Aiša piezvanīja uz norādīto numuru. Pēc neilga brīža atbildēja "tehniķis" – izklausījās, ka viņš ir profesionālis, – un apliecināja viņai, ka problēmu var novērst attālināti. Viņš lika viņai lejupielādēt "drošības programmatūru", kas ļāva viņam skenēt sistēmu. Aiša vēroja kā uz ekrāna parādās desmitiem viltotu "vīrusu". Tehniķis paskaidroja, ka viņas dators ir "būtiski inficēts", taču par vienreizēju 375 dolāru apmērā viņš to varot iztīrīt un pasargāt. Atvieglota Aiša samaksāja ar savu kredītkarti.
Tās pašas nedēļas beigās viņas kredītkartes izdevējs brīdināja viņu par vairākiem neatļautiem maksājumiem. Tajā brīdī Aiša saprata, ka draudzīgais "tehniskais atbalsts" patiesībā bija krāpnieki un ka tagad viņiem bija piekļuve ne tikai viņas kredītkartei, bet arī datoram.

Diemžēl Aišas stāsts ir ļoti izplatīts – tieši tā darbojas daudzi **tehniskā atbalsta krāpniecības** gadījumi.

Kas ir tehniskā atbalsta krāpniecība?

Tehniskā atbalsta krāpniecība notiek, kad noziedznieki pārliecina cilvēkus, ka ar viņu datoru, tālruni vai tiešsaistes kontu ir problēmas un ka ir nepieciešama tūlītēja "tehniskā atbalsta" palīdzība. Krāpnieki izliekas par likumīgiem uzņēmumiem vai iestādēm, piemēram, VID, policijai vai jūsu banku. Viņu mērķis? **Lai maldinātu jūs un izkrāptu naudu, iegūtu sensitīvu informāciju vai iegūtu attālināto piekļuvi kādai ierīcei, piemēram, jūsu datoram, telefonam vai kontiem.**

Šie krāpnieciskie mēģinājumi bieži sākas ar viltus pārlūka vai operētājsistēmas atjauninājuma paziņojumiem, tālruņa zvaniem vai īsziņām, kurās tiek apgalvots, ka jūsu dators ir inficēts vai jūsu konts ir kompromitēts. Neatkarīgi no tā, kā tās sākas, mērķis ir radīt paniku un likt jums noticēt, ka jāreaģē **nekavējoties**.

Ko viņi vēlas panākt?

Tehniskā atbalsta krāpniekus galvenokārt interesē trīs lietas:

1. **Jūsu nauda:** viņi pieprasa samaksu par "neeksistējošu problēmu" novēršanu – bieži pieprasot samaksu dāvanu kartes veidā, liekot veikt pārskaitījumus vai norēķināties kriptovalūtā, visām šīm metodēm kopīgs ir tas, ka tās ir grūti izsekojamas.
2. **Jūsu informācija:** viņi prasa jūsu datus - vārdu, uzvārdu, adresi, paroles vai bankas piekļuves informāciju it kā identitātes pārbaudei vai "atmaksas apstrādei".

3. **Piekļuve jūsu ierīcēm vai kontiem:** pārliecinot jūs instalēt attālinātās piekļuves programmatūru, viņi var izspiegot jūsu darbības, zagt datus vai instalēt īstu ļaunatūru, lai īstenotu turpmākus uzbrukumus.

Kā šī krāpniecība darbojas

Tehniskā atbalsta krāpniecība lielā mērā balstās uz **sociālo inženieriju**– manipulēšanu ar emocijām, lai radītu bailes un steidzamības sajūtu. Lūk, tipisks scenārijs:

1. **Viņi liek izjust bailes:** jūs redzat uznirstošo logu, saņemat īsziņu vai zvanu, kas apgalvo, ka jūsu sistēma vai konts ir apdraudēts. Ziņojumā tiek izmantoti satraucoši izteikumi, piemēram: "Jūsu dati tiks zaudēti!" vai "Jūsu konts tiks bloķēts!"
2. **Uzticības iegūšana:** krāpnieks uzdodas par profesionāli no labi zināma uzņēmuma, pat izmantojot oficiālus logotipus vai norādot viltotus tālruņu numurus.
3. **Piekļuve un maksājums:** viņi lūdz instalēt programmatūru vai noklikšķināt uz saites, kas tādējādi ļauj pieslēgties jūsu ierīcei. Pēc tam viņi pieprasa maksu par "labojumiem" vai "aizsardzības pakalpojumiem". Pat ja saprotat, ka tā ir krāpšana, un pārtraucat savienojumu, viņiem joprojām var būt piekļuve jūsu datiem.

Kā pasargāt sevi

1. **Saglabājiet mieru un domājiet kritiski:** īsti uzņēmumi **neparādīs** uznirstošos brīdinājumus ar tālruņa numuriem un nezvanīs jums bez iemesla. Ja kaut kas šķiet steidzams vai biedējošs, pārtrauciet darbības un pārbaudiet informāciju.
2. **Nezvaniet uz uznirstošajos logos redzamajiem telefona numuriem:** ja redzat brīdinājumu uznirstošajā logā, aizveriet pārlūku. Nereaģējiet uz tajā norādīto numuru vai saiti.
3. **Nepiešķiriet attālinātu piekļuvi:** nekad neļaujiet nepazīstamiem cilvēkiem piekļūt jūsu ierīcēm vai kontiem. Ja viņi sazinās ar jums un steidzina piešķirt piekļuvi, tā ir krāpšana.
4. **Uzraugiet un nodrošiniet savus kontus:** ja jums ir aizdomas, ka saskārāties ar krāpnieku, nekavējoties nomainiet paroles un pārbaudiet savus bankas kontus.

Noslēgumā

Tehniskā atbalsta krāpniecībā tiek izmantotas bailes, steiga un uzticēšanās — un tas var notikt ar jebkuru, neatkarīgi tehniskajām zināšanām. Ņemiet vērā: **Īsti uzņēmumi nekad nezvanīs, nesūtīs e-pastus un nerādīs uznirstošos logus, lūdzot attālinātu piekļuvi vai samaksu par problēmas novēršanu.** Miers un veselīgas skepses saglabāšana ir labākā aizsardzība.

Viesredaktore

Dženifera Koksa (Jennifer Cox) ir risinājumu konsultāciju direktore uzņēmumā "Tines", kas nodarbojas ar viedo automatizāciju un pārveido kiberdrošības darbības. Vairākkārt apbalvota kiberdrošības līdere, viņa ar aizrautību nodarbojas ar nākotnes nozares profesionāļu konsultēšanu un inovāciju, izcilības un iekļaušanas veicināšanu tehniskajās komandās globālajā kiberdrošības un automatizācijas ekosistēmā. https://www.linkedin.com/in/jennifermcox/

Resursi

Atjauninājumu spēks: https://www.sans.org/newsletters/ouch/power-updating/
Kā kibernoziedznieki izmanto jūsu emocijas: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
Paroļu frāžu spēks: https://www.sans.org/newsletters/ouch/power-passphrase/

Kopienai tulkoja: CERT.LV

Vairāk informācijas par Ouch! Varat atrast šajā saitē: https://www.sans.org/newsletters/ouch