OUCH! 2021. gada maijs

Ikmēneša informācijas drošības izdevums tev

Vikšķerēšana (Vishing) - tālruņa zvanu uzbrukumi un krāpšanās

Pārskats

Kad jūs mēģināt iztēloties kibernoziedznieku, jūs, iespējams, domājat par noziedzīgās pasaules ģēniju, kurš sēž pie datora un uzsāk pārdomātus uzbrukumus internetā. Kaut arī daži mūsdienu kibernoziedznieki patiešām izmanto progresīvas tehnoloģijas, daudzi vienkārši izmanto tālruni, lai apmānītu savus upurus. Tālruņa lietošanai ir divas lielas priekšrocības: Atšķirībā no citiem uzbrukumiem ir mazāk tehnoloģisku drošības risinājumu, kas var atklāt un apturēt ļaunprātīgu tālruņa zvanu; izmantojot tālruni, noziedzniekiem ir daudz vieglāk raisīt emocijas un radīt uzticību, kas atvieglo upuru apmānīšanu. Uzzināsim, kā pamanīt un apturēt šos uzbrukumus.

Kā darbojas tālruņa zvanu uzbrukumi?

Pirmkārt, jāsaprot, ka šie noziedznieki parasti vēlas iegūt jūsu naudu, informāciju vai piekļuvi jūsu datoram (vai visus trīs). Viņi to dara, apvārdojot jūs un panākot, ka izdarāt kaut ko tādu, ko jums nevajadzētu darīt; šo tehniku sauc par "sociālo inženieriju". Kibernoziedznieki bieži rada situācijas, kas telefonsarunas laikā šķiet ļoti steidzamas un reālas. Daži no visbiežāk sastopamajiem piemēriem:

- Zvanītājs izliekas, ka ir valsts iestādes pārstāvis, un informē jūs, ka jums ir nesamaksāti nodokļi. Viņi paskaidro, ka, ja jūs uzreiz nemaksāsiet nodokļus, jūs nokļūsiet cietumā, pēc tam pa tālruni spiež jūs samaksāt nodokļus ar kredītkarti. Šī ir krāpšana. Valsts iestādes oficiālus nodokļu paziņojumus nosūtīs tikai pa parasto pastu.
- Zvanītājs izliekas, ka ir no tāda uzņēmuma kā Amazon, Apple vai Microsoft Tech Support, un paskaidro, ka jūsu dators ir inficēts. Kad uzbrucēji pārliecina jūs, ka jūsu dators ir inficēts, viņi liek jums nopirkt viņu programmatūru vai piešķirt viņiem attālināto piekļuvi jūsu datoram.
- Automātiskais balss pasts informē, ka jūsu bankas konts vai kredītkarte ir anulēta, un jums ir jāatzvana uz numuru, lai to atkārtoti aktivizētu. Zvanot, jūs tiekat savienots ar automatizētu sistēmu, kas lūdz apstiprināt savu identitāti, kā arī uzdod dažādus privātus jautājumus. Šī tiešām nav jūsu banka. Viņi vienkārši reģistrē visu jūsu informāciju identitātes zādzības nolūkos.

Sargāt sevi

Vislabākā aizsardzība pret tālruņa zvana uzbrukumu esat jūs pats. Paturiet prātā šīs lietas:

- Vienmēr, kad kāds jums zvana un rada milzīgu steidzamības vai spiediena sajūtu, kļūstiet maksimāli piesardzīgs. Uzbrucēji cenšas panākt, lai steigā pieļaujat kļūdu. Pat ja sākotnēji tālruņa zvans šķiet pamatots, ja jums sāk šķist, ka kaut kas nav kārtībā, jebkurā laikā varat to pārtraukt un pateikt "nē"
- Īpaši jāuzmanās no zvanītājiem, kuri uzstāj, lai iegādājaties dāvanu kartes vai priekšapmaksas debetkartes.
- Nekad neuzticieties zvanītāja numuram. Uzbrucēji bieži vilto numurus, tāpēc izskatās, ka zvans tiek veikts no likumīgas organizācijas vai arī numuram ir tāds pats teritorijas kods kā jūsu tālruņa numuram.
- Nekad neļaujiet zvanītājam kaut vai īslaicīgi kontrolēt jūsu datoru un pierunāt jūs lejupielādēt kādu programmatūru. Šādi viņi var inficēt jūsu datoru.
- Ja vien jūs pats neesat veicis zvanu, nekad nesniedziet otrai pusei informāciju, kurai tai jau vajadzētu būt. Piemēram, ja jums piezvanīja no bankas, zvanītājam nevajadzētu lūgt jūsu konta numuru.
- Ja uzskatāt, ka tālruņa zvans ir uzbrukums, vienkārši pārtrauciet zvanu. Ja vēlaties noskaidrot, vai tālruņa zvans bija likumīgs, dodieties uz organizācijas tīmekļa vietni (piemēram, savas bankas tīmekļa vietni) un pats piezvaniet tieši uz klientu atbalsta tālruņa numuru. Tādā veidā jūs tiešām zināt, ka runājat ar īsto organizāciju.
- Ja pienāk tālruņa zvans no personas, kuru jūs personīgi nepazīstat, ļaujiet zvanam pāriet tieši uz balss pastu. Tādā veidā jūs varat pārskatīt nepazīstamus zvanus vēlāk. Vēl labāk, daudzos tālruņos varat to iespējot pēc noklusējuma, izmantojot funkciju "Netraucēt".

Krāpšanās un uzbrukumi pa tālruni pieaug. Jūs pats esat vislabākā aizsardzība uzbrucēju atklāšanā un apturēšanā.

Viesredaktors

Džena Foksa (Jen Fox) ir DEF CON 23 Black Badge īpašniece sociālās inženierijas kategorijā un kā drošības programmu speciāliste pasniedz drošības izglītības kursu "Domino". Atrodiet Dženu Twitter kā @j_fox.

Resursi

Sociālā inženierija: https://www.sans.org/security-awareness-training/resources/social-engineering-attacks
Teksta paziņojumu/ smikšķerēšanas uzbrukumi: https://www.sans.org/security-awareness-training/resources/social-engineering-attacks
Personalizēta krāpšana: https://www.sans.org/security-awareness-training/resources/personalized-scams
Ziņot par krāpšanos pa tālruni (ASV): https://www.reportfraud.ftc.gov

Kopienai tulkojis

OUCH! izdod SANS institūts programmas "Security Awareness" ietvaros un tas tiek izplatīts saskaņā ar Creative Commons BY-NC-ND 4.0 licences nosacījumiem. Jūs varat brīvi dalīties ar šo biļetenu vai izplatīt, kamēr 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).