OUCH!

SANS SECURITY AWARENESS

Ikmēneša informācijas drošības biļetens ikvienam

Uzmanību - zvana krāpnieks!

Pārskats

Domājot par kibernoziedzniekiem, parasti iztēlojamies ļaundarus, kas ar datora starpniecību veic izsmalcinātus uzbrukumus internetā. Kamēr daudzi mūsdienu ļaundari tiešām izmanto e-pastu vai ziņojumu apmaiņu, citi ir atraduši radošus veidus kā pielietot arī telefonu potenciālo upuru apmānīšanai. Telefona izmantošanai ir divi ievērojami labumi. Pirmkārt, eksistē daudz mazāk drošības tehnoloģiju, kas uzrauga telefona zvanus, nekā salīdzinoši tas ir, piemēram, e-pastiem. Otrkārt, izmantojot telefonu ļaundaris daudz labāk var „pārraidīt" savas emocijas, kas attiecīgi padara krāpniecību daudz efektīvāku. Tādēļ mēģināsim saprast, kā atpazīt un apturēt šādus uzbrukumus.

Kā darbojas telefona - krāpniecība?

Vispirms jāsaprot, ko uzbrucējs īsti vēlas? Parasti tā ir jūsu naudu, piekļuve jūsu datoram vai informācijai (vai visi trīs). Viņi to iegūst, jūs apmānot un panākot, ka neapzināti rīkojaties saskaņā ar viņu vēlmēm un plāniem. Šādi krāpnieciski zvani ir izplatīti visā pasaulē, un to mērķis ir radīt situācijas, kas šķiet steidzamas un ārkārtējas. Ļaundari caur iebiedēšanu vēlas „izsist" jūs no līdzsvara, apgrūtinot saprātīgu domāšanu, un tad piespiežot jūs kļūdīties. Daži piemēri:

Zvanītājs izliekas par nodokļu departamenta vai nodokļu iekasēšanas iestādes pārstāvi, un informē jūs par nenomaksātiem nodokļiem. Viņš paskaidro, ka nodokļu nenomaksāšanas gadījumā jums draud cietumsods, un mēģina piespiest jūs nosaukt kredītkartes datus pa telefonu. Šāda krāpniecības shēma ir populāra ASV, kaut arī realitātē ASV nodokļu iestādes nekad nezvana pašiem iedzīvotājiem. Parasti šādos gadījumos tiek nosūtīta parasta, oficiāla pasta vēstule.

Zvanītājs izliekas par Microsoft tehniskā atbalsta pārstāvi un paziņo, ka jūsu dators ir inficēts. Viltus pārstāvis ticami mēģina jūs pārliecināt par šķietami saķerto datorvīrusu, un tad piespiež jūs samaksāta par antivīrusa programmatūru vai arī pārliecina dot piekļuvi jūsu datoram. Realitātē īstais Microsoft parasti nezvana jums šādos gadījumos.

Jūs saņemat balss ziņojumu par to, ka jūsu bankas konts ir bloķēts un ka jums jāzvana uz noteiktu telefona numuru, lai to atbloķētu. Gadījumā, ja jūs tiešām piezvanāt, jums tiek uzdoti dažādi privāti dabas jautājumi - it kā, lai apliecinātu jūsu identitāti. Tā, protams, nav banka, bet gan ļaundari, kas ievāc informāciju, lai nozagtu jūsu identitāti.

Kā sevi pasargāt?

Jūs varat sevi pasargāt no šādiem uzbrukumiem, ievērojot sekojošo:

Katru reizi, kad kāds jums zvana un mēģina radīt satraukumu, esiet uzmanīgi. Arī tad, ja sākumā zvans šķiet patiess, bet pēc laika sāk šķist aizdomīgs, jums ir tiesības apstāties un pateikt "Nē".

Ja ir aizdomas, ka tā ir krāpniecība, vienkārši nolieciet klausuli. Ja vēlaties pārliecināties par zvana patiesumu, pārbaudiet informāciju attiecīgās iestādes (piemēram, bankas) mājas lapā, atrodiet klientu apkalpošanas tālruni un piezvaniet tiem paši. Tādejādi jūs varat būt droši, ka sadarbojaties ar īsto organizāciju.

Nekad pilnībā neuzticieties zvana noteikšanas funkcijai. Ļaudariem ir iespējas viltot tālruņa numuru tā, lai tas izskatītos pēc patiesās organizācijas numura vai arī ar tādu pašu valsts / reģiona kodu, kā jūsējais.

Nekad neļaujiet zvanītājam pārņemt jūsu datoru savā kontrolē, kā arī paši nekad neinstalējiet programmatūru pēc zvanītāja pieprasījuma. Tadā veidā jūs nodrošināt, ka ļaundarim zūd iespēja inficēt jūsu datoru.

Ja zvans nāk no kāda, ko jūs personīgi nepazīstat, ļaujiet zvanam nonākt balss pastkastītē. Pēc tam, kad ir brīvāks laiks, varat ar vēsu prātu pārskatīt nezināmos zvanus. Ja ir iespējams, uzstādiet šo funkciju telefonam jau pēc noklusējuma ar "Do not disturb" funkciju.

Krāpniecība, izmantojot telefonu izplatās. Jūs varat to atklāt un apturēt!

CERT.LV ir Latvijas Republikas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā. Uzziniet vairāk https://www.cert.lv vai sekojiet mums Twiterī @certlv.

Viesredaktors

Jen Fox *kā Vecākais drošības konsultants uzņēmumā All Covered nodrošinasociālās inženierijas, drošības izpratnes veicināšanas un risku novērtēšanas pakalpojumus. Jen ir sastopams arī Twitter kā @j_fox.*

Resursi

Informācija par identitāti, privātumu un tiešsaistes drošību:
https://www.consumer.ftc.gov/topics/privacy-identity-online-security
Ziņošana par krāpniecību ASV: https://www.ftccomplaintassistant.gov/#crnt
Sociālā inženierija: https://www.sans.org/u/Fi5

Redakcija: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Tulkojums: Edgars Tauriņš