SANS SECURITY AWARENESS

Teksta paziņojumu jeb smikšķerēšanas uzbrukumi

Pārskats

Viens no izplatītākajiem veidiem, kā kiberuzbrucēji cenšās apkrāpt vai apmānīt cilvēkus, ir krāpnieciski e-pasti (jeb pikšķerēšana) vai krāpnieciski telefona zvani. Taču, attīstoties tehnoloģijām, sliktie puiši izmēģina arvien jaunas metodes, cenšoties jūs apmānīt ar teksta paziņojumiem, tādiem kā īsziņas, iMessage, Facetime, WhatsApp, Slack vai Skype. Daži vienkārši paņēmieni sevis aizsardzībai un izplatītāko uzbrukumu atpazīšanai un novēršanai.

Kas ir teksta paziņojumu uzbrukumi?

Teksta paziņojumu uzbrukumos (jeb smikšķerēšanā, atvasinot no pikšķerēšanas) kiberuzbrucēji izmanto SMS vai citas ziņu sūtīšanas tehnoloģijas, lai sazinātos ar jums un panāktu, ka veicat darbības, kuras jums nevajadzētu veikt. Iespējams, viņi cenšās panākt, ka nospiežat uz kaitīgas saites, vai arī veicat telefona zvanu uz kādu noteiktu numuru, sniedzot viņiem jūsu bankas piekļuves informāciju. Tāpat kā tradicionālos pikšķerēžanas e-pastu uzbrukumos, sliktie puiši bieži izmanto emocijas, lai panāktu jūsu rīcību. Taču teksta paziņojumu uzbrukumus īpaši bīstamus padara tas, ka tie bieži šķiet daudz neformālāki vai personīgāki nekā e-pasti, palielinot iespēju, ka "iekritīsiet". Papildus tam, teksta paziņojumu uzbrukumos ir daudz mazāk informācijas un pavedienu, kas varētu jums palīdzēt pamantīt, ka kaut kas ir aizdomīgs vai nepareizs. Ja saņemat teksta paziņojumu, kas šķiet dīvains vai aizdomīgs, sāciet ar jautājumu sev, kāpēc es saņēmu šo ziņu, vai tas šķiet loģiski? Dažas izplatītākās uzbrukumu pazīmes.

Īpaša steidzamības sajūta, kad kāds mēģina jūs pasteidzināt uz darbību.

Vai saņemtajā ziņā tiek prasīta personīga rakstura informācija, paroles vai citi sensitīvi dati, pie kuriem citiem nevajadzētu būt piekļuvei?

Vai ziņa izklausās pārāk labi, lai būtu patiesa? Nē, jūs nevinnējāt loterijā, jo īpaši tajā, kurā nepieteicāties piedalīties.

Ja izskatās, ka ziņa sūtīta no kolēģa vai drauga konta vai telefona numura, taču galīgi neizklausās pēc viņiem, iespējams, ka viņu konts ir ticis uzlauzts, vai arī uzbrucējs cenšās izlikties par viņiem, lai panāktu jūsu rīcību.

Ja saņemat ziņu, kura jums raisa spēcīgas emocijas, nogaidiet mirkli, ļaujiet sev nomierināties un pārdomājiet visu, pirms atbildat.

Dažreiz sliktie puiši pat apvieno e-pasta un teksta ziņojumu uzbrukumus. Piemēram, šādi var izpausties krāpniecība ar dāvanu kartēm. Kiberuzbrucējs nosūtīs jums steidzamu e-pastu, izliekoties par draugu vai kolēģi, un lūgs jūsu telefona numuru. Tad uzbrucēji var sūtīt jums atkārtotus teksta ziņojumus un censties piespiest jūs iegādāties dāvanu kartes. Kad dāvanu kartes iegādātas, uzbrucēji liks jums nokasīt kodu no dāvanu karšu aizmugures un nosūtīt kodu attēlus viņiem. Cits izplatīts uzbrukumu veids ir aicinājums "ievērtēt" video vai attēlu (kuram “jūs neticēsiet!”), cenšoties raisīt jūsos ziņkārību. Ja izskatās, ka ziņu ir sūtījis kāds, kuru jūs pazīstat, pirms rīkojaties, piezvaniet un pārbaudiet.

Ja saņemat ziņu no kādas iestādes vai organizācijas un tā jums liekas dīvaina, sazinieties ar viņem un pārbaudiet. Piemēram, ja saņemat paziņojumu no savas bankas, kurā apgalvots, ka radušās problēmas ar jūsu kontu vai maksājumu karti, sazinieties ar banku pa tiešo, apmeklējot viņu mājas lapu vai zvanot uz telefona numuru, kas norādīts uz jūsu maksājumu kartes. Ņemiet vērā, ka lielākā daļa valsts iestāžu, tādas kā Valsts ieņēmumu dienests vai tiesībsargājošās institūcijas, nesazināsies ar jums teksta ziņojumu veidā.

Attiecībā uz teksta paziņojumu uzbrukumiem, jūs esat jūsu labākā aizsardzība.

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 *ir DEF CON 23 Black Badge īpašniece sociālās inženierijas ketegorijā un kā drošības programmu speciāliste pasniedz drošības izglītības kursu "Domino". Jūs varat sekot viņai Twitter @j_fox.*

Resursi

Sociālā inženierija:	http://www.sans.org/u/XAQ
Kā atpazīt pikšķerēšanu:	http://www.sans.org/u/XAV
Telefonkrāpniecība:	http://www.sans.org/u/XB0
Ziņot par krāpnieciskiem teksta paziņojumiem:	https://cert.lv/lv/kontakti

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 izplatīt šo biļetenu vai izmantot to savā informācijas tehnoloģiju drošības izglītošanas programmā ar nosacījumu, ka biļetens netiek izmainīts Papildu informācijai vai jautājumiem par tulkošanu izmantojiet www.sans.org/security-awareness/ouch-newsletter e-pasta adresi.
Redakcija: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Tulkojums: CERT.LV