Ikmēneša informācijas drošības izdevums tev

Pamaniet un pārtrauciet ziņojumapmaiņas uzbrukumus

Kas ir ziņojumapmaiņas uzbrukumi?

Smishing (hibrīdvārds, kas apvieno SMS un pikšķerēšanu) ir uzbrukumi, kas notiek, kad kiberuzbrucēji izmanto SMS, īsziņu sūtīšanas vai līdzīgas ziņojumapmaiņas tehnoloģijas, lai jūs apmānītu un liktu veikt darbības, kuras jums nevajadzētu veikt. Iespējams, viņi jūs apmāna un liek sniegt kredītkartes informāciju, zvanīt uz tālruņa numuru, lai iegūtu bankas informāciju, vai pārliecina jūs aizpildīt tiešsaistes aptauju, lai iegūtu jūsu personisko informāciju. Tāpat kā e-pasta pikšķerēšanas uzbrukumos, kibernoziedznieki bieži spēlē uz jūsu emocijām, lai liktu jums rīkoties, piemēram, radot steidzamības vai ziņkārības sajūtu. Tomēr ziņojumapmaiņas uzbrukumus tik bīstamus padara tas, ka tekstā ir daudz mazāk informācijas un mazāk norāžu nekā e-pastā, tāpēc jums ir daudz grūtāk noteikt, ka kaut kas nav kārtībā.

Izplatīta krāpniecība ir ziņojums, kurā teikts, ka esat laimējis iPhone, un jums tikai jānoklikšķina uz saites un jāaizpilda aptauja, lai to saņemtu. Patiesībā nekāda tālruņa nav, un aptauja ir paredzēta jūsu personiskās informācijas iegūšanai. Cits piemērs varētu būt ziņojums, kurā teikts, ka paku nevar piegādāt un norādīta saite uz vietni, kurā jums tiek lūgts sniegt informāciju, kas nepieciešama piegādes pabeigšanai, tostarp jūsu kredītkartes informāciju, lai segtu “pakalpojuma izmaksas”. Dažos gadījumos šīs vietnes var pat lūgt instalēt nesankcionētu mobilo lietotni, kas inficē un pārņem vadību pār jūsu ierīci.

Dažreiz kibernoziedznieki pat apvieno tālruņa un ziņojumapmaiņas uzbrukumus. Piemēram, jūs varat saņemt steidzamu īsziņu no bankas ar jautājumu, vai esat autorizējis neparastu maksājumu. Ziņojumā tiek lūgts atbildēt JĀ vai NĒ, lai apstiprinātu maksājumu. Ja jūs atbildēsit, kibernoziedznieks tagad zinās, ka esat gatavs iesaistīties, un piezvanīs jums, uzdodoties par bankas krāpšanas izmeklēšanas nodaļas darbinieku. Pēc tam viņi mēģinās no jums izvilināt jūsu finanšu un kredītkartes informāciju vai pat jūsu bankas konta piekļuves datus (lietotāju un paroli).

Ziņojumapmaiņas uzbrukumu pamanīšana un apturēšana

Šeit ir daži jautājumi, kas jāuzdod sev, lai pamanītu visbiežāk sastopamos pavedienus par ziņojumapmaiņas uzbrukumu:

- Vai ziņojums rada milzīgu steidzamības sajūtu, mēģinot jūs steidzināt vai piespiest rīkoties?

- Vai ziņojums novirza jūs uz vietnēm, kurās tiek prasīta jūsu personas informācija, kredītkartes, paroles vai cita sensitīva informācija, kurai viņiem nevajadzētu piekļūt?
- Vai ziņa izklausās pārāk labi, lai būtu patiesa? Nē, jūs patiešām nelaimējāt jaunu iPhone bez maksas.
- Vai saistītā vietne vai pakalpojums liek jums maksāt, izmantojot nestandarta metodes, piemēram, Bitcoin, dāvanu kartes vai Western Union pārskaitījumus?
- Vai ziņojumā tiek prasīts daudzfaktoru autentifikācijas kods, kas tika nosūtīts uz jūsu tālruni vai ģenerēts jūsu bankas lietotnē?
- Vai izskatās pēc kļūdaini nosūtītas ziņas? Ja tā, neatbildiet uz to un nemēģiniet sazināties ar sūtītāju; vienkārši izdzēsiet to

Ja saņemat ziņojumu no oficiālas organizācijas, kas jūs satrauc, zvaniet organizācijai tieši. Neizmantojiet ziņojumā iekļauto tālruņa numuru, tā vietā izmantojiet uzticamu tālruņa numuru. Piemēram, ja saņemat īsziņu no bankas, kurā teikts, ka ir problēma ar jūsu kontu vai kredītkarti, atrodiet uzticamu tālruņa numuru savas bankas tīmekļa vietnē, konta izrakstā vai bankas vai kredītkartes aizmugurē. Atcerieties arī, ka lielākā daļa valsts institūciju, piemēram, nodokļu vai tiesībsargājošo iestāžu, nekad nesazināsies ar jums, izmantojot īsziņu, tās sazināsies ar jums, izmantojot vecmodīgo pastu.

Runājot par ziņojumapmaiņas uzbrukumiem, jūs esat sava labākā aizsardzība.

Viesredaktors

Džefs Lomass (Jeff Lomas) ir Lasvegasas Metropoles policijas departamenta Kiberizmeklēšanas grupas detektīvs un pasniedz SANS SEC487 atvērtā pirmkoda izlūkdatu vākšanas un analīzes (OSINT) kursu. Džefs izmeklē augsto tehnoloģiju finanšu noziegumus, tostarp iejaukšanās biznesa e-pasta sarakstē, "smishing", šifrējošie izspeidējvīrusi (ransomware) un sarežģītas kriptovalūtas zādzības, kā arī naudas "atmazgāšanas" lietas.

Resursi

Apturi pikšķerēšanu: https://www.sans.org/newsletters/ouch/stop-that-phish/
Sociālā inženierija: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Vishing: telefoniski uzbrukumi un krāpniecība: https://www.sans.org/newsletters/ouch/vishing

Tulkojums: CERT.LV