OUCH! 2024. gada jūlijs

Ikmēneša informācijas drošības izdevums tev

Teksta ziņojumapmaiņas uzbrukumi: Smikšķerēšanas sāga

Marks bija neizpratnē par ziņu – paziņojumu par paku piegādi no Amazon – “Piegāde neizdevās! Noklikšķiniet uz saites tagad, lai izvēlētos atkārtotas piegādes laiku, pretējā gadījumā jūsu paka tiks nosūtīta atpakaļ.” Marks nevarēja atcerēties, ka pēdējā laikā būtu kaut ko pasūtījis internetā, bet, godīgi sakot, viņš pasūtīja tik daudz lietu internetā, ka bija viegli aizmirst. Nevēloties palaist garām nevienu sūtījumu, viņš noklikšķināja uz saites, un tika ielādēta lapa, kurā tika lūgts sniegt kontaktinformāciju, “lai nodrošinātu atkārtotu piegādi”. Ziņa šķita mazliet dīvaina, bet Marks nolēma, ka labāk būt drošam nekā nožēlot. Viņš ievadīja savas mājas adreses datus, un tad viņam tika pieprasīta papildinformācija, tostarp kredītkartes informācija. Uzticoties uzņēmumam, viņš ievadīja visu, ko tas lūdza, lai nodrošinātu piegādi. Pēc tam lapā tika parādīts paziņojums, ka viņa paka drīzumā tiks piegādāta. Pēc piecpadsmit minūtēm Marks saņēma zvanu no kredītkaršu uzņēmuma, kas viņam paziņoja, ka viņa karte tiek izmantota, lai veiktu daudzus maksājumus tiešsaistē visā pasaulē. Marks sastinga, jo saprata, ka nekādas paciņas nav un ka ziņa ir bijusi krāpšana, lai izvilinātu no viņa visu informāciju, tostarp kredītkartes datus.

Kas ir Smikšķerēšanas uzbrukumi?

Ziņojumapmaiņas uzbrukumi, ko dēvē arī par smikšķerēšanu (vārdu "SMS" un "pikšķerēšana" kombinācija), notiek, kad kiberuzbrucēji izmanto SMS, īsziņas, vai līdzīgas ziņojumapmaiņas tehnoloģijas, lai ar viltu piespiestu veikt darbības, kuras nevajadzētu veikt, piemēram, izpaust kredītkartes vai bankas konta paroli vai instalēt viltotu mobilo lietotni. Tāpat kā e-pasta pikšķerēšanas uzbrukumos, kibernoziedznieki bieži cenšas radīt jūsos noteiktas emocijas, piemēram, radot steidzamības vai ziņkārības sajūtu. Tomēr ziņojumapmaiņas (sms) 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.

Dažreiz kibernoziedznieki kombinē tālruņa un ziņojumapmaiņas uzbrukumus. Piemēram, jūs varat saņemt steidzamu īsziņu no bankas ar jautājumu, vai esat autorizējis neparastu maksājumu. Ziņojumā tiek lūgts atbildēt uz ziņu ar JĀ vai NĒ. Ja jūs atbildēsiet, kibernoziedznieks 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 (lietotājvārdu un paroli).

Ziņojumapmaiņas uzbrukumu - smikšķerēšanas pamanīšana un apturēšana

Dažas no izplatītākajām smikšķerēšanas uzbrukuma pazīmēm:

- **Steidzamība**: jebkura ziņa, kas rada milzīgu steidzamības sajūtu, kad kāds cenšas jūs steidzināt vai izdarīt spiedienu, lai veiktu kādu darbību, piemēram, apgalvojot, ka jūsu konti tiks slēgti vai nonāksiet cietumā.
- **Mantkārība**Vai ziņa izklausās pārāk labi, lai būtu patiesa? Nē, jūs patiešām neesat laimējis jaunu iPhone bez maksas.
- **Šaubas**: Ja saņemat ziņu, kas izskatās kā "nepareizā numura" ekvivalents vai kāds, kuru nepazīstat, vienkārši saka "Sveiks!", neatbildiet uz to un nemēģiniet sazināties ar sūtītāju; vienkārši izdzēsiet to. Tie ir kibernoziedznieku mēģinājumi uzsākt ar jums sarunu, iespējams, ka tas ir sākums romantiskai krāpšanai.
- **Personīgā informācija**Vai saņemtā ziņa novirza jūs uz vietnēm, kurās tiek prasīta jūsu personas informācija, kredītkartes, paroles vai cita sensitīva informācija, kurai viņiem nevajadzētu piekļūt?
- **Maksājumi**: Ļoti aizdomīgi izturieties pret neparastiem maksājumu pieprasījumiem, piemēram, naudas sūtīšanu, izmantojot "Western Union" vai "Bitcoin".

Ja saņemat sms no oficiālas organizācijas, kas, jūsuprāt, varētu būt leģitīma, zvaniet, lai pārbaudītu ziņu uz konkrētās iestādes oficiālo tālruni. Neizmantojiet sms iekļauto tālruņa numuru, tā vietā izmantojiet uzticamu - oficiālu tālruņa numuru. Piemēram, ja saņemat sms no bankas, kurā teikts, ka ir problēma ar jūsu kontu vai kredītkarti, atrodiet savas bankas oficiālo tālruņa numuru tās tīmekļa vietnē, konta izrakstā vai kredītkartes otrā pusē. 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 smikšķerēšanas uzbrukumiem, jūs pats sevi varat aizsargāt vislabāk.

Viesredaktors

Destineja Plaza (Destiney Plaza) ir kiberdrošības inženiere Kārnegija un Melona (Carnegie Mellon) Universitātes Programmatūras inženierijas institūtā. Viņai patīk iedvesmot gan iesācējus, gan kiberdrošības profesionāļus, uzstājoties ar lekcijām dažādās auditorijās. Viņai ir sertificētas informācijas sistēmu drošības speciālistes sertifikāts, bakalaura grāds datorzinātnēs un maģistra grāds vadības informācijas sistēmās.

Resursi

Ziņojumapmaiņa: ko drīkst un ko nedrīkst darīt: https://www.sans.org/newsletters/ouch/messaging-dos-and-donts/
Pārtraukt tālruņa zvanu krāpšanu: https://www.sans.org/newsletters/ouch/stop-phone-call-scams/
Emocionālie ierosinātāji – kā kiberuzbrucēji piemāna cilvēkus: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

Tulkojums: CERT.LV