Ikmēneša informācijas drošības izdevums tev

Pikšķerēšanas uzbrukumi kļūst viltīgāki

Pikšķerēšanas uzbrukumi ir kļuvuši par izplatītāko metodi, ko kiberuzbrucēji izmanto pret cilvēkiem darbā un mājās. Pikšķerēšanas uzbrukumi tradicionāli ir e-pasta vēstules, ko sūta kiberuzbrucēji, lai jūs pierunātu darīt kaut ko tādu, ko nevajadzētu darīt, piemēram, atvērt inficētu e-pasta vēstules pielikumu, noklikšķināt uz ļaunprātīgas saites vai izpaust savu paroli. Lai gan tradicionālie pikšķerēšanas uzbrukumi notiek arī mūsdienās, daudzi kiberuzbrucēji veido uzlabotas pikšķerēšanas e-pasta vēstules, kas ir pielāgotākas un grūtāk atklājamas. Viņi izmanto arī tādas tehnoloģijas kā īsziņas, sociālos medijus vai pat tālruņa zvanus, lai jūs iesaistītu viņu krāpšanā un apmānītu. Lūk, viņu jaunākie triki un padomi, kā tos pamanīt.

Kiberuzbrucēji ir informēti

Kādreiz pikšķerēšanas e-pasta vēstules bija vieglāk atklāt, jo tās bija vispārīgas ziņas, kas izsūtītas miljoniem nejauši izvēlētu cilvēku. Kiberuzbrucējiem nebija ne jausmas, kas varētu kļūt par upuriem; viņi vienkārši zināja, ka, jo vairāk e-pasta vēstuļu viņi nosūtīs, jo vairāk cilvēku viņi varēs apmānīt. Šos vienkāršākos uzbrukumus bieži varēja atklāt, meklējot neparastus e-pasta ziņojumus ar "Cienījamais klient!" sākumā, pareizrakstības kļūdām vai ziņojumiem, kas izklausījās pārāk labi, lai būtu patiesi, piemēram, Nigērijas prinči jums piedāvā miljoniem dolāru.

Mūsdienu kiberuzbrucēji ir daudz gudrāki. Tagad viņi izpēta savus topošos upurus, lai izveidotu pielāgotāku uzbrukumu. Tā vietā, lai nosūtītu pikšķerēšanas e-pasta vēstuli pieciem miljoniem cilvēku vai nosūtītu tādas, kas izskatītos pēc vispārīgām e-pasta vēstulēm, ko sūta korporācijas, uzbrucēji to var nosūtīt tikai pieciem cilvēkiem un pielāgot uzbrukumu tā, lai izskatītos, ka to sūta kāds pazīstams cilvēks. Kiberuzbrucēji to dara šādi:

- pētot mūsu LinkedIn profilus, to, ko publicējam sociālajos tīklos, vai izmantojot publiski pieejamu vai tumšajā tīmeklī atrodamu informāciju.
- izveidojot ziņojumus, kas šķietami nāk no vadības, kolēģiem vai piegādātājiem, kurus pazīstat un ar kuriem strādājat.
- uzzinot, kādi ir jūsu hobiji, un nosūtot jums ziņu, izliekoties par kādu, kam ir kopīgas intereses ar jums.
- uzzinot, ka nesen esat apmeklējis konferenci vai atgriezies no ceļojuma, un pēc tam sagatavojot e-pasta vēstuli, kurā piemin to.

Kiberuzbrucēji aktīvi izmanto citas metodes, lai nosūtītu tos pašus ziņojumus, piemēram, sūtot īsziņas vai pat zvanot tieši pa tālruni.

Kā atpazīt šos modernākos pikšķerēšanas uzbrukumus

Tā kā kiberuzbrucēji nesteidzas un izpēta savus plānotos upurus, šos uzbrukumus var būt grūtāk pamanīt. Labā ziņa ir tā, ka jūs joprojām varat tos pamanīt, ja zināt, ko meklējat. Pirms atbildat uz aizdomīgu ziņojumu, uzdodiet sev šādus jautājumus:

1. Vai vēstījums rada pastiprinātu steidzamības sajūtu? Vai uz jums tiek izdarīts spiediens apiet jūsu organizācijas drošības politiku? Vai jūs steidzina pieļaut kļūdu? Jo lielāks spiediens vai steidzamības sajūta, jo lielāka iespēja, ka notiek uzbrukums.
2. Vai e-pasta vēstule vai ziņojums ir saprotams? Vai jūsu uzņēmuma vadītājs steidzami sūtītu jums ziņu ar lūgumu palīdzēt? Vai jūsu vadītājam tiešām ir nepieciešams, lai jūs steigtos nopirkt dāvanu kartes? Kāpēc bankai vai kredītkaršu uzņēmumam būtu jāpieprasa personiskā informācija, kurai jau būtu jābūt tam pieejamai? Ja ziņojums šķiet dīvains vai nevietā, iespējams, tas ir uzbrukums.
3. Vai saņemat ar darbu saistītu e-pasta vēstuli no uzticama kolēģa vai, iespējams, sava vadītāja, bet e-pasta vēstulē ir izmantota personīgā e-pasta adrese, piemēram, @gmail.com?
4. Vai esat saņēmis e-pasta vēstuli vai ziņojumu no kādas pazīstamas personas, bet ziņojuma formulējums, tonis vai paraksts ir nepareizs un neparasts?

Ja ziņojums šķiet dīvains vai aizdomīgs, tas var būt uzbrukums. Ja vēlaties pārliecināties, vai e-pasta vēstule vai ziņojums ir uzticams, viena no iespējām ir piezvanīt personai vai organizācijai, kas jums sūta ziņojumu, izmantojot uzticamu tālruņa numuru.

Jūs esat vislabākā aizsardzība. Izmantojiet veselo saprātu.

Viesredaktors

Fils Hofmans (Phil Hoffman) ir daļēji pensionējies IT konsultants ar 40 gadu pieredzi infrastruktūras un drošības jomā. Viņš ir ilggadējs OUCH! korespondents un redaktors, kā arī aizraujas ar tehnoloģijām, riteņbraukšanu un fotografēšanu.

Resursi

Sociālā inženierija: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Trīs populārākie krāpniecības veidi: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Krāpšana ziņojumapmaiņā: https://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
Tālruņa zvanu krāpniecība: https://www.sans.org/newsletters/ouch/vishing/
Izlūkošana ar atklāti pieejamu informācijas avotu palīdzību: https://www.sans.org/newsletters/ouch/search-yourself-online/

Tulkojums: CERT.LV