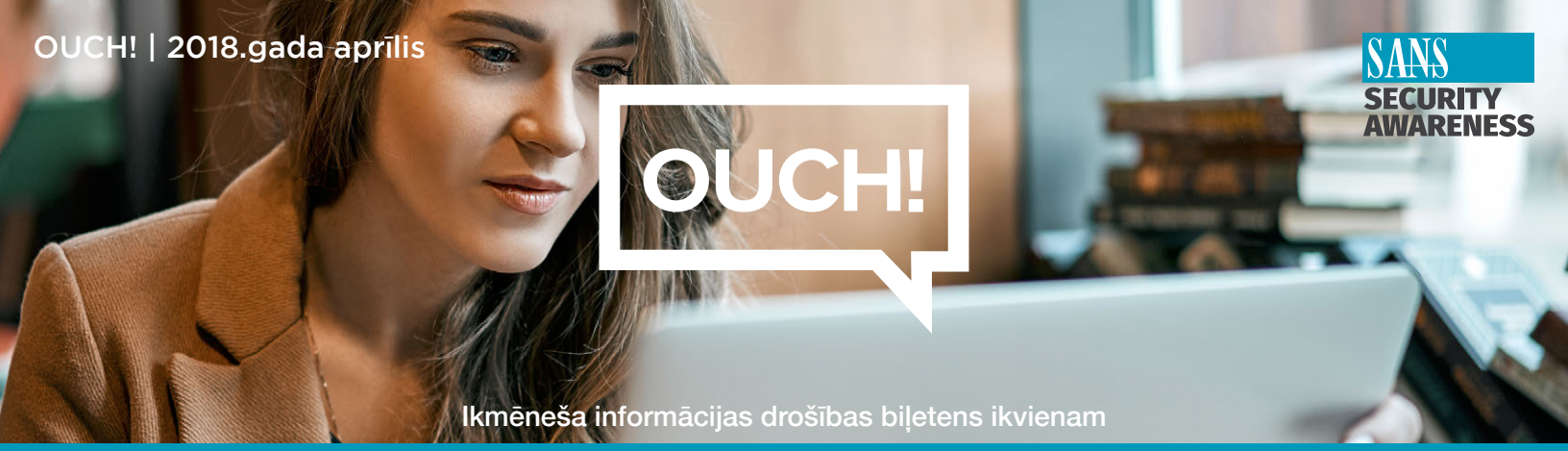

Ikmēneša informācijas drošības biļetens ikvienam

Kā atpazīt pikšķerēšanu

Pārskats

E-pasta un ziņu apmaiņas pakalpojumi (Skype, Twitter,Snapchat u.c.) ir vieni no populārākajiem mūsdienu saziņas līdzekļiem. Mēs tos izmantojam katru dienu gan darba vajadzībām, gan arī saziņai ar draugiem un ģimeni. Ņemot vērā faktu, ka tik plaša sabiedrības daļa paļaujas uz šiem saziņas līdzekļiem, tos labprāt pikšķerēšanas uzbrukumiem izmanto arī kibernoziedznieki. Šodien noskaidrojot, kas tieši slēpjas zem nosaukuma „pikšķerēšana", jūs varēsiet nākotnē daudz vieglāk atpazīt un apturēt šos uzbrukumus kā darba vietā, tā arī mājās.

Kas ir pikšķerēšana?

Pikšķerēšana ir uzbrukuma veids, kas, izmantojot e-pastu vai ziņu apmaiņas programmas, mēģina jūs apmuļķot un mudina veikt darbības, kas kaitē jums pašiem, piemēram, nospiest kādu saiti, atklāt savu paroli vai atvērt inficētu e-pasta pielikumu. Uzbrucēji cenšas padarīt šīs ziņas pēc iespējas pārliecinošākas un ticamākas, kā arī cenšas izprovocēt uz emocijām balstītu atbildes reakciju, piemēram, steigu vai ziņkārību. Uzbrucējs var izveidot ziņu tā, lai izskatītos, ka tā nāk no kāda jums pazīstama cilvēka vai uzņēmuma, kura pakalpojumus jūs regulāri izmantojat. Iespējams, var tikt pievienots pat jūsu bankas logo vai arī viltota nosūtītāja e-pasta adrese, lai ziņa šķistu ticamāka. Uzbrucēji šādas ziņas nosūta miljoniem cilvēku. Parasti gan viņi nezin, kurš tieši uzķersies, taču paļaujas uz principu, ka jo vairāk ziņu tiks izsūtīts, jo lielāka ir iespēja, ka kāds tomēr uzķersies.

Kā sevi pasargāt?

Vairumā gadījumu, pēc e-pasta atvēršanas un izlasīšanas nekas ļauns nenotiek. Lai klasiskais pikšerēšanas uzbrukums nostrādātu, uzbrucējam nepieciešama kāda jūsu papildu darbība. Eksistē pazīmes, pēc kurām var konstatēt uzbrukumu, zemāk uzskaitītas izplatītākās:

- Tiek radīta milzīga steiga, nepieciešamība rīkoties nekavējoties - pirms nav noticis kaut kas slikts, piemēram, īstenoti draudi slēgt jūsu kontu vai ielikt jūs cietumā. Uzbrucējs vēlas jūs steidzināt, lai jūs pieļautu kļūdas.
- Tiek radīts papildu spiediens, lai jūs pārkāptu darba drošības noteikumus vai neievērotu citkārt ierastas darba procedūras.
- Tiek raisīta ziņkārība, vai arī tiek piedāvāts kaut kas, kas izklausās pārāk labi, lai būtu patiesība (nē, jūs nevinnējāt loterijā).

- Tiek izmantotas lietišķas un vispārināmas uzrunas formas, piemēram, “Cienījamais klient”. Vairums kompāniju vai draugu uzrunās jūs personiskāk.
- Tiek pieprasīta ļoti sensitīva informācija, piemēram, kredītkartes numurs / parole vai jebkāda cita informācija, ko leģitīms sūtītājs jau tāpat zinātu.
- Ziņojums tiek sūtīts it kā no oficiālas organizācijas, bet e-pasta adrese izmantota privātā, piemēram, „@gmail.com” vai arī tekstā ir daudz gramatikas kļūdu.
- Ziņojums šķietami nāk no oficiāla e-pasta (piemēram, jūsu priekšnieka), bet Reply-To adrese norāda uz kādu privāto e-pasta adresi.
- Jūs saņemat ziņu no kāda, ko jūs pazīstat, bet ziņas „rokraksts” vai noformējums neatbilst līdzšinējai komunikācijai. Ja jums radušās aizdomas, piezvaniet sūtītājam, pārliecinieties, ka ziņa tiešām nāk no viņa. Kiberuzbrucējam ir samērā vienkārši izveidot ziņu, kas izskatās tā, it kā tā nāktu no drauga vai kolēģa.

Aicinām ievērot sniegtos ieteikumus, lai padarītu savu tiešsaistes pieredzi daudz drošāku un patīkamāku. Lai uzzinātu vairāk par to, kā droši izmantot sociālos tīklus vai ziņot par nepieļaujamām aktivitātēm, izpētiet attiecīgā sociālā tīkla drošības sadaļu.

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

Tonia Dudley piedāvā pašas izstrādātas Drošības informēšanas programmas jau kopš 2011. gada, tostarp viņa ir radījusi arī godalgotu pretpikšķērēšanas apmācību programmu. Plašāka informācija par Tonia Dudley pieejama šeit: www.linkedin.com/in/toniadudley.

Resursi

Sociālā inženierija:	https://www.sans.org/u/Cb1
Palīdzība aizsargājot citus:	https://www.sans.org/u/Cb6
E-pasta ieteikumi:	https://www.sans.org/u/Cbg
CEO krāpšana:	https://www.sans.org/u/Cbl
OUCH! Tulkojumi un arhīvs:	https://www.sans.org/u/Cbq

License

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