Ikmēneša informācijas drošības izdevums tev

Emocionālie ierosinātāji – kā kiberuzbrucēji piemāna cilvēkus

Pārskats

Kiberuzbrucēji pastāvīgi izgudro jaunus veidus, kā cilvēkus pierunāt darīt to, ko nevajadzētu darīt, piemēram, klikšķināt uz ļaunprātīgām saitēm, atvērt inficētus e-pasta pielikumus, iegādāties dāvanu kartes vai izpaust savas paroles. Turklāt viņi bieži izmanto dažādas tehnoloģijas vai platformas, lai mēģinātu citus apmānīt, piemēram, e-pastu, tālruņa zvanus, īsziņas vai sociālos medijus. Lai gan tas viss var šķist satraucoši, lielākajai daļai šo uzbrukumu ir kopīga viena un tā pati iezīme – emociju ekspluatēšana. Zinot kiberuzbrucēju izmantotos emocionālos ierosinātājus, bieži vien varat pamanīt viņu uzbrukumus neatkarīgi no izmantotās metodes.

Emocijas ir būtiskākais elements

Viss sākas ar emocijām. Cilvēki pārāk bieži pieņem lēmumus, pamatojoties uz emocijām, nevis faktiem. Patiesībā par šo jēdzienu ir izveidota vesela pētījumu joma, ko dēvē par "uzvedības ekonomiku" un kuru vada tādi pētnieki kā Daniels Kanemans (Daniel Khaneman), Ričards Tālers (Richard Thaler) un Kass Sanšteins (Cass Sunstein). Par laimi, ja mēs zinām, kādus emocionālos ierosinātājus ievērot, varam veiksmīgi pamanīt un apturēt lielāko daļu uzbrukumu. Turpmāk ir uzskaitīti visbiežāk sastopamie emocionālie ierosinātāji, kas jāievēro. Dažkārt kiberuzbrucēji vienā e-pasta vēstulē, īsziņā, ierakstā sociālajos tīklos vai tālruņa zvanā izmanto dažādu emociju kombināciju, tādējādi padarot kiberuzbrukumu daudz efektīvāku.

Steidzamība: Steidzamības iespaida izraisīšana ir viens no visbiežāk sastopamajiem emociju ierosinātājiem, jo tas ir ļoti efektīvs. Kiberuzbrucēji bieži izmanto bailes, trauksmi, nepietiekamību vai iebiedēšanu, lai pamudinātu jūs kļūdīties. Piemēram, saņemat steidzamu e-pasta vēstuli no savas priekšnieces, kurā pieprasīts nekavējoties nosūtīt viņai sensitīvus dokumentus, lai gan patiesībā tas ir kiberuzbrucējs, kas uzdodas par jūsu priekšnieci. Vai arī saņemat īsziņu no kiberuzbrucēja, kas uzdodas par valsts iestādes pārstāvi, ar paziņojumu, ka jūsu nodokļu nomaksa ir nokavēta un jums ir jāveic tūlītēji maksājumi, citādi jūs ieslodzīs cietumā.

Dusmas: Jūs saņemat ziņu par kādu politisku, vides vai sociālu jautājumu, kas jums ir ļoti svarīgs, piemēram, "Jūs neticēsiet, ko dara šī politiskā grupa vai korporatīvais uzņēmums!"

Pārsteigums / **Ziņkārība**: Dažreiz uzbrukumos, kas ir visveiksmīgākie, sniegts vismazāk informācijas. Ziņkārība ir saistīta ar pārsteigumu; mēs vēlamies uzzināt vairāk. Tā ir reakcija uz kaut ko negaidītu. Piemēram, kiberuzbrucējs jums nosūta ziņu, ka sūtījums nav piegādāts, un lūdz, lai noklikšķināt uz saites, lai uzzinātu vairāk, lai gan jūs neko neesat pasūtījis tiešsaistē. Mūs vilina iespēja uzzināt vairāk! Diemžēl saite nesatur nekādu informāciju par sūtījumu, tai ir tikai ļaunprātīgs nodoms.

Uzticība: Uzbrucēji mēdz izmantot vārdu vai zīmolu, kam uzticaties, lai pārliecinātu jūs veikt kādu darbību. Piemērs šādai situācijai ir ziņa, kurā kāds uzdodas par jūsu banku, labi zināmu labdarības organizāciju, uzticamu valdības organizāciju vai pat pazīstamu personu. Tas, ka e-pastā vai īsziņā ir izmantots jums zināmas organizācijas nosaukums un logotips, nenozīmē, ka ziņojums patiešām ir saņemts no šīs organizācijas.

Patīkams satraukums: No bankas vai pakalpojumu sniedzēja saņemat īsziņu ar pateicību par savlaicīgu maksājumu veikšanu. Pēc tam īsziņā tiek sniegta saite, kurā varat saņemt balvu – jaunu iPad. Cik aizraujoši! Saite ved uz tīmekļa vietni, kas izskatās oficiāla, bet pieprasa visu jūsu personisko informāciju vai norāda, ka jums ir jāsniedz kredītkartes informācija, lai segtu nelielas piegādes/pārvadāšanas izmaksas. Šajā situācijā darbojas kiberuzbrucējs, kas vienkārši nozog jūsu naudu vai identitāti.

Empātija / līdzjūtība: Kiberuzbrucēji izmanto jūsu labo gribu. Piemēram, pēc tam, kad ziņās pieminēta kāda katastrofa, viņi izsūta miljoniem viltus e-pasta vēstuļu, izliekoties par labdarības organizāciju, kas vēlas palīdzēt cietušajiem, un lūdz jums naudu.

Labāk izprotot šos emocionālos ierosinātājus, jūs būsiet daudz labāk sagatavoti, lai pamanītu un apturētu kiberuzbrucējus neatkarīgi no viņu izmantotās viltības, tehnoloģijas vai platformas.

Viesredaktors

My-Ngoc Nguyen ir “Secured IT Solutions” izpilddirektors/galvenais direktors. Viņai ir 20 gadus ilga pieredze kiberdrošības un riska pārvaldības programmu vadīšanā un pilnveidošanā gan federālajā valdībā, gan privātajā sektorā. Viņa ir sertificēta pasniedzēja, kas regulāri pasniedz “MGT512”. https://www.linkedin.com/in/menop, My-Ngoc Nguyen | “SANS” institūts @“MenopN”.

Resursi

Sociālā inženierija: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Krāpšana pa tālruni: https://www.sans.org/newsletters/ouch/vishing/
Krāpšana sociālajos tīklos: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Krāpšana ziņojumapmaiņā: https://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
Pikšķerēšanas uzbrukumi: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/

Tulkojums: CERT.LV