Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

Sukčiavimas, apsimetant įmonės vadovu, arba kompromitavimas verslo laiškais

Kaip yra sukčiaujama, apsimetant įmonės vadovu, arba kompromituojama verslo laiškais?

Kibernetiniai nusikaltėliai vis tobulina sukčiavimo, apsimetant įmonės vadovu, arba kompromitavimo verslo laiškais technikas. Tai tiksliniai, el. paštu atliekami nusikaltimai, siekiant įtikinti auką, imtis veiksmų, kurių ji neturėtų imtis. Daugeliu atvejų, blogiukai siekia gauti pinigų. Šie nusikaltimai yra itin pavojingi todėl, kad prieš nusikaltimą, kibernetiniai nusikaltėliai pirmiausiai ieško informacijos apie savo aukas. Taip pat todėl, kad saugumo technologijos negali sustabdyti šių nusikaltimų, kadangi el. laiškuose nėra prisegta jokių virusais užkrėstų priedų arba pateikiama nuorodų į kenkėjiškas svetaines. Štai kaip vykdomi šie nusikaltimai.

Kibernetiniai nusikaltėliai pirmiausiai internetu ieško informacijos apie nusižiūrėtą auką ir su kokiais žmonėmis ji bendrauja. Pavyzdžiui, jei jie nusitaikytų į jus, tuomet jie nustatytų, kas yra jūsų tiesioginis vadovas, o galbūt nekilnojamojo turto agentas, su kuriuo bendradarbiaujate dirbdami iš namų. Tuomet kibernetinis nusikaltėlis parašo el. laišką, apsimesdamas vienu iš tų žmonių ir jį išsiunčia jums. El. laiškas yra pažymimas kaip skubus, o jame reikalaujama nedelsiant imtis tokių veiksmų, kaip apmokėti sąskaitą, pakeičiant mokėjimo gavėją arba esate įtikinami atsiųsti konfidencialius dokumentus. Tokiu el. laišku yra siekiama sukelti spaudimą, kad padarytumėte tai, ko jie prašo. Štai pora pavyzdžių, kaip gali būti vykdomas toks nusikaltimas.

Bankinis pavedimas. Kibernetiniai nusikaltėliai siekia gauti pinigų. Jie nustato, kokioje įmonėje dirbate ir kas dirba jos buhalterijoje arba kas yra atsakingas už pavedimų darymą. Tuomet nusikaltėliai tiems asmenims parašo ir išsiunčia el. laišką, apsimesdami jų tiesioginiu arba įmonės vadovu. El. laiške yra rašoma, kad tai yra nenumatytas, skubus atvejis ir kad pinigai turi būti pervesti į naują banko sąskaitą nedelsiant. Tokiu el. laišku yra siekiama sukelti spaudimą, kad žmogus suklystų, tuo tarpu realybėje pinigai būtų siunčiami kibernetiniam nusikaltėliui.

Sukčiavimas mokant mokesčius. Kibernetiniai nusikaltėliai siekia pasisavinti žmonių asmeninę informaciją, kad galėtų sukčiauti mokant mokesčius. Vienas iš greičiausių būdų tai padaryti yra pavogti visų įmonės darbuotojų informaciją. Kibernetiniai nusikaltėliai ieško ir nustato, kas dirba žmogiškųjų išteklių skyriuje. Tuomet išsiunčia suklastotus el. laiškus, apsimesdami įmonės vadovu arba kuo nors iš teisės skyriaus. El. laiškuose sukuriama neatidėliotinos skubos istorija, kad turi būti nedelsiant pateikta visų darbuotojų mokesčių informacija. Žmogiškųjų išteklių skyriuje dirbantys darbuotojai galvoja, kad jie konfidencialius dokumentus siunčia įmonės vadovui, bet realiai jie juos siunčia kriminaliniam nusikaltėliui.

Kaip apsisaugoti?

Taigi ką galėtumėte padaryti, kad apsisaugotumėte? Geriausia jūsų apsauga yra sveikas protas. Štai keletas dažniausių užuominų, į kurias turėtumėte atkreipti dėmesį.

El. laiškas yra labai trumpas, bet skubus (dažnai jį sudaro vos keli sakiniai), o iš parašo galima spręsti, kad jis buvo atsiųstas iš mobilaus įrenginio.

Yra jaučiamas didelis skubinimas ir spaudimas ignoruoti arba apeiti savo darbdavio taikomą politiką. Visada vadovaukitės su darbu susijusia politika ir procedūromis net, jei atrodo, kad el. laišką atsiuntė jūsų vadovas ar net generalinis direktorius.

El. laiškas yra susijęs su darbu, tačiau siunčiamas iš asmeninio el. pašto adreso, kurio galūnė dažnai būna @gmail.com arba @hotmail.com.

Atrodo, kad el. laišką atsiuntė įmonės vadovas, bendradarbis arba jūsų pažįstamas pardavėjas, tačiau žinutėje naudojamas bendravimo tonas jų neprimena.

Yra pateikti mokėjimo nurodymai, kurie skiriasi nuo tų, kuriuos jau esate gavę, pavyzdžiui, prašoma nedelsiant padaryti pavedimą į visiškai kitą banko sąskaitą.

Jei įtariate, kad į jus darbe kreipėsi kibernetinis nusikaltėlis, nustokite su juo bendrauti ir praneškite apie tai savo tiesioginiam vadovui. Jei į jus kibernetinis nusikaltėlis kreipėsi namie arba tapote auka, padariusia tokį mokėjimo pavedimą, nedelsdami apie šį atvejį praneškite savo banko darbuotojams, o tuomet teisėsaugos pareigūnams.

Kviestinis redaktorius

Donald Cavender *yra buvęs FTB specialusis agentas, turintis daugiau nei 22 metus patirties skaitmeninės ekspertizės ir kibernetinių nusikaltimų srityse. Neseniai, dirbdamas Vašingtono kompromitavimo elektroniniais laiškais tyrimų koordinatoriumi, jis pradėjo nustatinėti kibernetinių nusikaltimų organizacijas. Taip pat jis rengia mokymus ir atlieka mokslinius tyrimus skaitmeninės ekspertizės ir kibernetinių tyrimų srityse.* @don_cavender
https://www.linkedin.com/in/donald-cavender

Šaltiniai

Socialinė inžinerija:	https://www.sans.org/u/HE3
Sustabdykite tokią duomenų vagystę:	https://www.sans.org/u/HE8
Sustabdykite tokią kenkimo programinę įrangą:	https://www.sans.org/u/HEd
Apsaugokite savo paskyras:	https://www.sans.org/u/HEi