Mėnesinis informacinio saugumo naujienlaiškis Tau

Individualizuoti apgaulingi laiškai

Apžvalga

Kibernetiniai nusikaltėliai sugalvoja vis naujesnių ir kūrybiškesnių būdų, kaip apkvailinti žmones. Šiuo metu populiarėja nauja apgaulės rūšis – individualizuotų apgaulingų laiškų siuntimas. Radę arba įsigiję informacijos apie milijonus žmonių, jie šią informaciją panaudoja suasmenintiems nusikaltimams vykdyti. Toliau papasakosime, kaip veikia nusikaltimo schema, kurioje yra naudojami tokie apgaulingi laiškai, ir pateiksime dažniausiai pasitaikančius pavyzdžius. Kuo daugiau žinosite apie šiuos apgaulingus laiškus, tuo lengviau jums bus juos atpažinti ir nuo jų apsisaugoti.

Kaip visa tai vyksta?

Sukčiavimas el. paštu ar telefono skambučiais nėra naujiena, kadangi kibernetiniai nusikaltėliai daugybę metų bando apgauti vis daugiau žmonių. Tokius pavyzdžius apima antraštė „Sveikiname laimėjus loteriją!“ arba prastai pagarsėjusi „Nigerijos princo“ apgaulė, kurios metu sukčius aukai pažada sumokėti didelę pinigų sumą, jeigu ji padės ją atsiimti, jam pervesdama nedidelę pinigų sumą, kurią gavęs jis dingsta arba sugalvoja papildomų mokesčių. Tačiau šiais tradiciniais sukčiavimo atvejais, kibernetiniai nusikaltėliai nežino su kuo jie bendrauja. Šiuo atveju, jie paprasčiausiai sukuria bendro pobūdžio pranešimą ir jį išsiuntinėja milijonams žmonių. Kadangi tokie apgaulingi laiškai tinka bet kam, juos įprastai yra labai lengva atpažinti. Individualizuotas apgaulingas laiškas skiriasi tuo, kad kibernetiniai nusikaltėliai pirmiausiai apie žmogų paieško informacijos ir nusižiūrėtai aukai sukuria asmeniškai pritaikytą tekstą. Jie tai atlieka susirasdami arba įsigydami duomenų bazę, kurią sudaro žmonių vardai, pavardės, slaptažodžiai, telefonų numeriai ar kiti asmeniniai jų duomenys. Tokią informaciją lengva gauti iš visų svetainių, į kurias buvo įsilaužta. Taip pat ją galima rasti socialiniuose tinklalapiuose ir viešai prieinamuose valstybinių įstaigų archyvuose. Toliau nusikaltėliai gali susisiekti su visais asmenimis, kurių informaciją jiems pavyko gauti.

Vienas iš populiariausių kibernetinių nusikaltėlių naudojamų triukų yra baimės sukėlimas arba išpirkos reikalavimas, siekiant asmenį priversti jiems sumokėti pinigus. Tokia nusikalstama veikla yra atliekama taip. Jie randa arba įsigyja informaciją, kurią sudaro naudotojų vardai ir slaptažodžiai, gauti iš svetainių, į kurias buvo įsilaužta. Tokioje duomenų bazėje jie randa jūsų paskyros informaciją ir jums (bei visiems kitiems, esantiems toje duomenų bazėje) išsiunčia po el. laišką, kuriame įrašo keletą jūsų asmeninių duomenų, įskaitant jūsų susikurtą slaptažodį, gautą iš svetainės, į kurią buvo įsilaužta. Nusikaltėliai jūsų slaptažodį pateikia kaip „įrodymą“, kad buvo įsilaužta į jūsų asmeninį kompiuterį arba kitą įrenginį, kas iš tikrųjų yra netiesa. Tuomet nusikaltėlis teigia, kad įsilaužęs į jūsų kompiuterį taip pat pastebėjo, kad internete žiūrite pornografinius vaizdo įrašus. Galiausiai, el. laiške yra grasinama, kad jei jiems nesumokėsite išpirkos, jie šios internetinės veiklos įrodymais pasidalins su jūsų šeimos nariais ir draugais.

Visa apgaulingo laiško gudrybė yra ta, kad beveik visais tokiais atvejais kaip šis, kibernetinis nusikaltėlis niekada nebūna įsilaužęs į jūsų įrenginio sistemą. Jis net nežino, kas jūs esate arba kokiose svetainėse lankotės. Apgaulingų laiškų siuntėjas paprasčiausiai bando pasinaudoti keliais gautais jūsų asmeniniais duomenimis, siekdamas jus įbauginti ir įtikinti, kad jis buvo įsilaužęs į jūsų kompiuterį arba kitą įrenginį, ir priversti jus sumokėti jam pinigus. Prisiminkite, jog blogiukai tokią pačią metodiką gali naudoti ir sukčiaudami telefonu.

Ką turėčiau daryti?

Supraskite, kad tokie el. laiškai ar telefono skambučiai kaip šie yra apgaulingi. Natūralu bijoti, kai kažkas turi jūsų asmeninę informaciją. Tačiau prisiminkite, kad siuntėjas jums meluoja. Tokia ataka yra automatiškai atliekamo, didžiulio masto nusikalstamo plano dalis, o ne bandymas jus asmeniškai sukompromituoti. Šiais laikais kibernetiniams nusikaltėliams yra žymiai lengviau rasti arba įsigyti asmeninę informaciją, todėl tikėkitės tokių apgaulingų laiškų ateityje gauti vis daugiau. Štai keletas užuominų, į kurias turėtumėte atkreipti dėmesį:

⚠

- **gavę itin skubų el. laišką, žinutę ar telefono skambutį, būkite itin įtarūs. Jei kas nors jums bando sukelti tokias emocijas, kaip baimė ar skubos jausmas, jie jus bando priversti suklysti.**
- **gavę reikalavimą sumokėti bitkoinais, dovanų kuponais ar kitais neatsekamais būdais.**
- **gavę įtartiną el. laišką, „Google“ svetainėje paieškokite, ar yra kitų žmonių pranešimų apie tokias atakas.**

Galiausiai, geriausia jūsų apsauga yra sveikas protas. Taip pat rekomenduojame kiekvienoje iš savo paskyrų susikurti po unikalų ir ilgą slaptažodį. Neprisimenate visų savo slaptažodžių? Tuomet naudokite slaptažodžių tvarkytuvę. Be to, įjunkite dviejų etapų asmens tapatybės patvirtinimą ten, kur tai įmanoma padaryti.

Kviestinis redaktorius

Lenny Zeltser *yra kibernetinio saugumo veteranas. Įmonėje „Minerva Labs“ jis kuria sprendimus, padedančius apsisaugoti nuo kenkimo programų, o „SANS“ institute veda paskaitas apie saugumą. Taip pat jis turi patirties saugumo valdymo ir konsultavimo paslaugų teikimo srityse. Jo veiklą galite stebėti svetainėje* zeltser.com/blog *ir „Twitter“ paskyroje* zeltser.com/blog.

Šaltiniai

Socialinė inžinerija:	https://www.sans.org/u/MUU
Sustabdykite sukčiavimą:	https://www.sans.org/u/MUZ
Paieškokite informacijos apie save internete:	https://www.sans.org/u/MV4
Slaptažodžių tvarkytuvės:	https://www.sans.org/u/MV9