Küberpetuskeemid meelitavad psühholoogiliste nõksudega osavalt välja nii andmeid kui raha

6 aastat tagasi - 02.10.2019 Autor: AM

Internetis levivad õngitsuskirjad ja petuskeemid on läinud juba väga osavaks ja usutavaks ning neist on saanud omaette äriliik, kus virtuaalmaailma kurikaelad püüavad õngitseda inimeste väärtuslikke andmeid või meelitada neid raha üle kandma. Petuskeemid varjavad endas põhjalikult läbimõeldud psühholoogiat, mille abil inimlikke nõrkusi ära kasutatakse. Millele kurikaelad rõhuvad, kui üritavad inimesi „haneks tõmmata“, räägib Elisa ärikliendiüksuse juht ning juhatuse liige Margus Vaino.

Gmail blokeerib ligi 100 miljonit õngitsuskirja päevas. Kõigele lisaks on Google´i avaldatud andmete järgi Gmaili poolt blokeeritud *phising*- ehk õngitsuskirjadest 68% uued variatsioonid, mida pole varem nähtud.

Phising ehk andmepüük või kalastamisrünne on teatud tüüpi internetipettus, mille eesmärgiks on saada teada inimeste isiklikke või diskreetseid andmeid illegaalselt raha teenimise eesmärgil.

Kuidas seda tehakse?

Andmepüük toimub siis, kui usaldusväärseks isikuks maskeerunud ründaja petab ohvri avama e-kirja, sotsiaalmeediasõnumit või lühisõnumit. Seejärel meelitatakse ohver vajutama pahatahtlikule lingile, mis võib viia pahavara paigaldamisele arvutis, avada arvuti lunavararünnakule või viia tundliku info avaldamisele.

Kuigi kontseptsioon on lihtne, siis arenevad sarnased andmepüügi meetodid pidevalt. Möödas on ajad, mil raha jagas rikas prints Nigeeriast või teavitati üllatuslikust pärandusest varalahkunud Kanada onult. Skeemid on läinud kompleksemaks, intelligentsemaks ja inimlikumaks ning on mõnikord vägagi usutavad.

Kõige lihtsam on selliste pettuste toimimisest rääkida läbi näidete.

Mõne firma raamatupidajale või personalitöötajale saadetakse kiri, kus palutakse kõrgema ülemuse poolt kiirelt raha kanda ühele kontole või muidu võib ettevõtte jaoks juhtuda midagi väga halba. Esmapilgul võib tunduda tõesti, et kirja saatis ülemus, kes palub sind näiteks nimeliselt ja kuna olukord tundub olevat tõsine, tahab üldjuhul iga töötaja käituda sellises olukorras kiirelt ja operatiivselt. Tegelikult võib aga juhi konto olla pahalaste poolt kaaperdatud või on tegu lihtsalt e-kirjaga, mis on väga sarnane ülemuse omaga.

See e-kiri mõjub töötajale aga mitmel erineval viisil, mis võib kallutada teda mõtlematult ülekannet tegema:

- **Võimusuhte ja autoriteedi esile toomine**

Sarnane kiri tuleb alati kõrgemalt ülemuselt või juhilt ning seda eesmärgil, et töötaja tunneks tööalast kohustust kuulata ülemuse palvet. Mõnikord lisatakse kirjale juurde ka inimlik palve, et näiteks ta unustas seda teha, nüüd on kontorist väljas ja kohe-kohe peab olema arve makstud. Inimestena püüame me ikka üksteist mõista ja võimalusel appi tulla.

- **Kiirus**

Alati on õngitsuskirjad seotud lühikese ajalise piiranguga. Raha on vaja kiirelt üle kanda, andmeid on vaja kärmesti uuendada või tasuta pakutavast tootest on alles viimased eksemplarid. Kiiruse faktor on oluline, et inimene kaotaks valvsuse ja ei asuks teksti süvitsi analüüsima.

- **Emotsionaalne mõju**

Emotsionaalsel tasandil kirjaga sideme saavutamine on üks mõjukaimaid viise, kuidas inimene konksu otsa saada. Sarnastel juhtudel seotakse õngitsus näiteks heategevuse ja kahjutunde tekitamisega või rõhutakse hoopis inimese ahnusele ning kasu saamise motiivile.

Alati aga ei soovitagi kohe raha saada. Nagu on paljud eestlased omal nahal tundnud, siis piisab ka sellest, kui sisestad oma telefoninumbri valesse kohta ja juba oled liitunud igakuise teenusega, mis sulle mitte midagi ei anna, aga mille eest küsitakse paar eurot kuus. Äsja levis ka Smart-ID andmeõngitsus, kus paluti e-posti teel uuendada andmeid.

Petuskeemid on pidevas arengus ja kogu aeg otsitakse uusi viise, kuidas inimeste varale või andmetele ligi pääseda. Ühelt poolt üritatakse aina tihedamatest *phising* filtritest mööda pääseda ja teisalt millegi uuega inimeste postkasti pääseda, sest uute skeemide kohta puuduvad inimestel teadmised ning kogemused.

Siiski selgub Google´i poolt läbiviidud uuringust, et 45% inimestest ei tea või ei mõista, mis on andmepüük ja õngitsuskiri. Vähene teadlikus probleemist suurendab oluliselt andmepüügi riski ja võib piirata kasutajate seas ennetavate meetmete rakendamist.

Kuidas ennetada ohvriks langemist?

Näiteks tabas Elisat mõni aeg tagasi rünnak, kus ründajad kehastasid ühte ettevõtte juhti ja saatsid korrektses eesti keeles kirja, milles palusid vahetada kontonumbrit, millele laekub juhi palk. Kasutati juhi nime ja esmapilgul tundus, et isegi korrektset e-posti aadressi. Tegelikkuses oli tegu aga osava võltsinguga.

Üheks vastumeetmeks oleks see, kui ettevõte rakendaks avalduste ja teiste dokumentide digitaalset allkirjastamist. Nii on alati kindel, et dokumendi või avalduse esitaja on ka tegelikult ise selle taga.

Kõige parem viis andmepüügi ennetamiseks on inimeste ja töötajate harimine, et nad aru saaksid, millega on tegu, kuidas seda tuvastada ja kuidas end kaitsta. Sellele lisaks on soovituslik kõigil kasutada, kus vähegi võimalik, kaheastmelist autentimist. See muudab kasutajate kontode kompromiteerimise oluliselt keerukamaks ja kasutajate jaoks kasutamise turvalisemaks.

Vaata lisaks:

- https://security.googleblog.com/2019/08/understanding-why-phishing-attacks-are.html
- https://elie.net/talk/deconstructing-the-phishing-campaigns-that-target-gmail-users/

- Uudised

- Turvalisus

Pilt