Patarimai padėsiantys atpažinti pavojingą laišką

Elektroninis paštas - vienas paprasčiausių ir pigiausių būdų platinti kenksmingą programinę įrangą. Kasdieninėje veikloje naudojamas elektroninis paštas tampa neatsiejama darbo dalimi, kuri gali sukelti rūpesčių jei kompiuterio naudotojas bus neatidus ir pasielgs neatsargiai. Norėdami supažindinti naudotojus su galimais pavojais, pateikiame keletą elektroninių laiškų bruožų, kurie turėtų sukelti įtarimą.

Ypač svarbu, kad gavęs laišką kompiuterio naudotojas neveiktų impulsyviai, nespaustų pateiktų nuorodų, neatidarinėtų prisegtų failų, o ramiai įvertintų situaciją: "ar tikrai laiškas motyvuotai adresuotas man?", "ar žinutė neatrodo per daug dirbtinė?". Neapgalvotai atliktas veiksmas gali užkrėsti Jūsų kompiuterį kenksmingu kodu, kuris galimai vogs Jūsų informaciją, slaptažodžius ar net pinigus.

Paprastai piktavaliai stengiasi pasinaudoti socialinės inžinerijos metodais ir bando: sukelti smalsumą arba išgasdinti naudotoją, kad šis nesusimąstęs padarytų klaidą (paspaustų nuorodą ar atidarytų prisegtą failą).

Įtartino laiško bruožai:

1. Siuntėjas Jums nėra žinomas, laiško nelaukėte, tačiau laiške stengiasi sudaryti tokį įspūdį - kreipiasi itin familiariai arba itin oficialiai. Prie kreipinio derinama ir sugalvota istorija: "Sveikas, čia nuotraukos iš..." arba "Gerb. Pavardė, tai dokumentas, kurio Jūs prašėte".
2. Kreipiniui naudojama Jūsų elektroninio pašto adreso dalis (automatinių siuntimo sistemų bruožas). Pavyzdžiui: "Gerb. vardas.pavarde, siunčiu Jums..." arba "Sveikas, vardas.pav, čia nuotraukos iš susitikimo...".
3. Laiško antraštė arba turinyje pateikiama nuoroda žada parodyti sensacingas nuotraukas arba supažindinti su svarbia informacija ("intymios įžymybių nuotraukos" arba "paviešinti svarbūs dokumentai"). Deja, bet piktavaliai tam tikslui labai greitai išnaudoja ir įvairias skaudžias nelaimes ("rasto sudužusio lėktuvo nuotraukos", "nusikaltimai žmogiškumui vykstančiame konflikte").
4. Prašoma skubiai perskaityti ir pateikti atsakymą ar nuomonę apie prisegtą dokumentą ar nurodytą tinklapį.
5. Laiško tekstas parašytas laužyta lietuvių ar užsienio kalba, matote linksnių/galūnių ir kitų gramatinių klaidų, jaučiama logikos stoka. Kadangi lietuvių kalba yra gramatiškai sudėtinga, šis bruožas padeda identifikuoti laiškus, kuriuos siuntė užsienio šalių piktavaliai, pasinaudoję automatinio vertimo programomis.
6. Viliojama "neįtikėtinomis akcijomis ir nuolaidomis", informuojama apie laimėjimą ir kviečiama pranešti "kur persiųsti prizą", siūlomi "nemokami žaidimai" ar filmukai. Pavyzdžiui: "Nigerijos

laiškai", kuriuose kalbama apie daugelio milijonų palikimą, kuriuo su Jumis nori pasidalinti arba prašo pagalbos padedant pervesti didelę sumą pinigų iš trečiojo pasaulio šalies. Atsakius į tokius laiškus, sukčiai Jūsų prašys pateikinėti įvairius asmeninius duomenis arba pervesti pinigų "smulkioms transakcijoms".

7. Įspėja apie "pasibaigusį slaptažodžio galiojimo laiką" ir kviečia "prisijungti ČIA, kad jį pakeistumėte". Ypatingai pavojingi laiškai, kurių siuntėjai tikisi išgasdinti naudotoją ir priversti atsidaryti svetainę (kurios dizainas bus nukopijuotas ir mėgdžios tikrosios svetainės išvaizdą), pateikti savo prisijungimo vardus ir slaptažodžius. Ši informacija gali būti panaudota Jūsų privataus elektroninio pašto paskyrų (angl. account) ar elektroninėje sąskaitoje esančių pinigų pasisavinimui. Svarbu atsiminti, jog niekas neturi teisės klausti Jūsų slaptažodžių (nei telefonu, nei paštu, nei gyvai) - nesvarbu ar jie prisistato kompiuterių tinklo administratoriumi, ar padalinio vadovu, ar kitu pareigūnu.
8. Laiške prašoma persiųsti informaciją "10 draugų per ateinančias x valandų". Tokie grandininiai laiškai ne tik be reikalo apkrauna tarnybines pašto stotis, tačiau ir platina gandus, išgalvotas, gavėjus gąsdinančias, istorijas, bet ir gali išplatinti Jūsų elektroninio pašto adresą (po keleto persiuntimų draugo draugui) ir jis bus įtrauktas į šlamšto gavėjų (gausite daug šlamšto) ar siuntėjų (Jūsų adresą blokuos sistemos) sąrašą.

Štai keletas tipinių pavojingų laiškų pavyzdžių:

1. Apgaulingas laiškas siekiantis sudominti naudotoją ir priversti jį atidaryti svetainę (kurioje gali slėptis kenksmingas kodas arba prašymas įvesti savo prisijungimo duomenis). Atsiųstas iš pavogtos gmail pašto dėžutės. Ypatingai pavojinga jei siunčiama toje dėžutėje esantiems kontaktiniams asmenims - kadangi adresatai mano, jog žino iš ko atėjo laiškas, pasitiki siunčiamu turiniu.

Nedidelė gudrybė - gavus panašų laišką, galima užvesti pelės rodyklę ant pateiktos nuorodos (**BET JOS NESPAUSTI**, o palaukti kol pasirodys informacinė lentelė), matoma, kad nuoroda veda ne į žadamą google dokumentų talpyklą, bet kitą adresą.

2. Analogiškas apgaulingas laiškas, tik šį kartą naudojamas automatinės programos pagalba išverstas tekstas (matomos vertimo ir gramatikos klaidos). Užvedus pelės rodyklę (**BET JOS NESPAUDŽIANT**, o palaukus kol pasirodys informacinė lentelė) matoma, jog nuoroda veda visai ne į google talpyklą.

3. Šia laiške naudojami pavogti asmens duomenys, kurie gali būti visiškai teisingi, tačiau naudojami be asmens sutikimo. Analogiška situacija su pateikta nuoroda. Svarbu atsiminti, kad elektroninis adresas iš kurio atsiųstas laiškas nėra joks įrodymas - į pašto dėžutę gali būti įsibrauta pavogiant jos prisijungimo duomenis arba dėl nesaugaus pašto serverio imituota neegzistuojančios pašto dėžutės adresas (pvz.: vardas[@]pasauliovaldovas.lt)

From: [redacted]kaite@kempinski.com>
To:
Cc:
Subject: Hello

Hello,

Please view the document i uploaded for you online,

Sign In with your email to view the document its very important.

The document might not open properly on old browser, make sure you are on Firefox or Chrome browser.

Kind Regards
People Oriented

With regards,

[redacted]
Front Office Manager

Kempinski Hotel Cathedral Square Vilnius
Universiteto str. 14
LT-01122, Vilnius
Lithuania.

Tel: +370 5 220 1115
Fax: +370 5 220 1120

[redacted]e@kempinski.com

http://www.voc[redacted]/
includes/include1/login-victorzs-h.html
Click to follow link