OUCH! | Joulukuu 2015

Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

Kalastelu

Yleiskatsaus

Sähköposti on nykyisin yleisin kommunikaatioväline, jota käytämme päivittäiseen työskentelyyn, sekä tuttujen ja perheen kanssa kommunikoimiseen. Lisäksi yritykset käyttävät sähköpostia verkkopalveluiden tarjoamisessa, kuten verkko-ostosten varmistamiseen. Koska sähköposti on niin suuressa roolissa kaikkien ihmisten päivittäisessä elämässä, sähköpostista on myös tullut tärkein hyökkääjien hyväksikäyttämä työkalu. Tässä uutiskirjeessä käymme läpi, miten hyökkääjät käyttävät kalastelua osana hyökkäyksiä ja miten voit suojautua sitä vastaan.

Vierastoimittaja

Tohtori Lance Hayden toimii vastaavana johtajana Berkeley Research Group - yrityksessä. Hän on erikoistunut turvallisuuskulttuuriin ja –käyttäytymiseen ja on ollut kirjoittamassa McGraw-Hill-kustantajan julkaisemaa “People-Centric Security: Transforming Your Enterprise Security Culture”- kirjaa. Löydät Lancen Linkedinistä **www.linkedin.com/in/drhayden**.

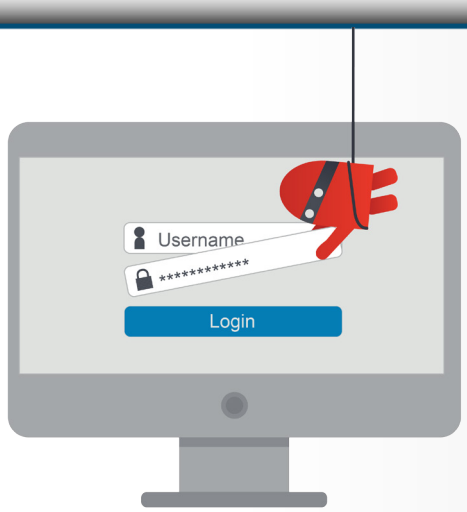
Kalastelu

Kalastelu viittaa hyökkäykseen jossa hyökkääjä käyttää sähköpostia, viestintäsovellusta tai sosiaalista mediaa saadakseen käyttäjän tekemään tiettyjä asioita, esim. klikkaamaan tiettyä linkkiä tai avaamaan liitetiedoston. Käyttäjä tehdessä hyökkääjän haluaman asian hyökkääjällä on mahdollisuus päästä käsiksi käyttäjän luottamuksellisiin tietoihin tai saastuttaa käyttäjän kone haittaohjelmalla. Kalasteluviestit ovat kehittyneet viime aikoina merkittävästi ja kalasteluviesti saattaa näyttää erittäin uskottavalta tai siltä, että sen on lähettänyt joku käyttäjälle luotettava lähettäjä, kuten tuttu henkilö tai yritys. Viesteihin lisätään tunnettuja logoja ja lähettäjän osoite saatetaan väärentää näyttämään täysin asianmukaiselta. Koska hyökkääjät tietävät, että kovin moni ei viesteihin reagoi, valmis kalasteluviesti lähetetään tuhansille henkilöille, koska hyökkääjälle riittää, jos edes muutama henkilö saadaan reagoimaan ja mitä useammalle viestin lähettää, sitä useampi onnistuminen saadaan vastaukseksi. Kalastelu vastaa verkoilla kalastamista, et voi olla koskaan varma mitä verkkoihin osuu, mutta mitä isompi verkko, sitä enemmän siihen kaloja jää yleensä kiinni. Hyökkääjät käyttävät kalastelua lukuisiin eri tavoitteisiin:

- **Tiedon kerääminen**: Hyökkääjän tavoitteena on kerätä luottamuksellisia tietoja, kuten salasanoja, luottokorttinumeroita tai pankkitietoja. Kalasteluviesti sisältää yleensä linkin, joka vie sinulle tunnetun näköiselle sivulla jossa sinua pyydetään syöttämään luottamuksellisia tietoja, jotka menevät suoraan hyökkääjälle.
- **Haitalliset linkit**: Hyökkääjän tavoitteena on saada laitteesi haltuunsa lähettämällä kalasteluviestin joka sisältää linkin. Linkistä avautuva sivusto sisältää haittaohjelman, joka käyttää hyväkseen laitteesi haavoittuvuuksia. Kun laitteesi sisältää haavoittuvuuden, siihen asentuu haittaohjelma, joka saastuttaa koneesi hyökkääjän haluamalla tavalla.

Kalastelu

- **Haitalliset liitteet**: Hyökkääjän tavoitteet ovat samat kuin yllä, mutta linkin sijaan haittaohjelma on viestin liitteenä ja sen avatessa haittaohjelma asentuu koneelle.
- **Huijaukset**: Ihmisiä on aina huijattu erinäisten huijareiden toimesta ja kalastelua käytetään digiaikana huijareiden työkaluna. Viestissä hyväntekeväisyysjärjestö haluaa sinulta jotakin apua, tai joku kertoo, että olet voittanut jotain. Kaikissa näissä tapauksissa viesteihin vastattua, yleensä seuraava askel on se, että sinulta pyydetään rahaa, jotta asiassa päästään eteenpäin. Tosiasiassa et koskaan saa mitään takaisin vaan menetät rahasi.



Paras keinosi puolustautumiseen on terve järki. Jos viesti epäilyttää tai on liian hyvää ollakseen totta, suhtaudu siihen varauksella.

Itsesi suojaaminen

Useimmissa tapauksissa sähköpostien avaaminen tai lukeminen ei voi aiheuttaa mitään seuraamuksia. Jotta kalasteluyritys toimisi, hyökkääjän pitää saada käyttäjä tekemään tiettyjä asioita. Käyttäjän onneksi, kalasteluviesteissä on yleensä tiettyjä vinkkejä, joista voi päätellä viestin asiattomuuden:

- Sähköpostissa vaaditaan nopeita toimia ja usein näihin liittyy jonkinlainen uhkaus, eli käyttäjältä odotetaan jotain toimia jottei jotain, kuten tilin sulkemista tapahdu. Hyökkääjät haluavat, että käyttäjä toimii nopeasti eikä ajattele asiaa enempää kuin on pakko.
- Saamasi viesti sisältää liitteen jota et odottanut tai viestissä kannustetaan liitteen avaamiseen. Hyvänä esimerkkinä on viesti jonka liitetiedostossa luvataan tietoja yrityksesi irtisanomisiin tai palkkoihin liittyen tai että sinua syytetään jostakin ja lisätietoja on linkissä.
- Nimesi sijaan viesti alkaa yleisellä lausahduksella, kuten arvoisa asiakas. Useimmat sinulle viestejä lähettävät tahot tietävät nimesi.
- Sähköpostissa pyydetään luottamuksellisia tietoja, kuten luottokortin tietoja tai salasanoja.
- Viesti vaikuttaa tulleen asianmukaisesta organisaatiosta, mutta kieliasu on huono tai viestissä on kirjoitusvirheitä. Lisäksi viesti saattaa tulla yleisestä päätteestä, kuten @gmail.com, @yahoo.com tai @hotmail.com.
- Linkki näyttää oudolta tai epäviralliselta. Yksi hyvä vinkki on pitää hiiren osoitinta linkin päällä painamatta sitä, kunnes ohjelma näyttää linkin todellisen osoitteen. Jos tämä näytetty osoite eroaa linkin osoitteesta, älä seuraa linkkiä. Mobiililaitteissa voit pitää sormeasi linkin päällä nähdäksesi samat tiedot.

Kalastelu

- Saamasi viesti on tullut luotettavalta lähettäjältä, mutta kieliasu tai tyyli ei vaikuta täysin oikealta. Jos epäilet, että viesti ei ole oikeasti siltä jolta se näyttää olevat, soita lähettäjälle ja varmista. Viestin lähettäjän väärentäminen on äärettömän helppoa.

Terveen järjen käyttö on paras keino varautua kalastelua vastaan ja jos uskot, että viesti on kalastelua, yksinkertaisinta on vain poistaa se.

LUE LISÄÄ

Liity kuukausittaisen OUCH! tietoturvatietoisuus-uutiskirjeen postituslistalle, lue OUCH! arkistoja ja tutustu SANS-järjestön muihin tietoturvatietoisuuteen liittyviin ratkaisuihin osoitteessa http://www.securingthehuman.org.

Elisa Appelsiini on korkean osaamisen IT-palvelutalo. Noin 400 IT-alan ammattilaisen voimin tuotamme monipuolisia ja tietoturvallisia tietotekniikkaan liittyviä pilvi-, työn tuottavuus-, konsultointi- ja ulkoistuspalveluja. Kehitämme myös asiakkaidemme liiketoimintaa tukevia sovelluksia ja tuotteita. Toimintamme perustuu syvään teknologiaosaamiseen ja aidosti asiakaslähtöiseen toimintaan.

Elisa Appelsiini is a comprehensive IT service provider owned by the leading provider of communications services in Finland, Elisa. Elisa Appelsiini helps its customers to enhance their business and increase competitiveness by offering high-end IT services in consulting, cloud, integration, software development and outsourcing.

Lähteet

Sosiaalinen hakkerointi:	https://www.securingthehuman.org/ouch/2014#november2014
Viisi askelta turvallisuuteen:	https://www.securingthehuman.org/ouch/2014#october2014
Minut hakkeroitiin, mitä nyt?:	https://www.securingthehuman.org/ouch/2014#may2014
OnGuard Online:	https://www.onguardonline.gov/phishing
SANS Päivän tietoturvavinkki:	https://www.sans.org/tip_of_the_day.php

Lisenssi

 Toimitus: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Käännös suomeksi: Kirill Filatov, CISO, Elisa Appelsiini Oy