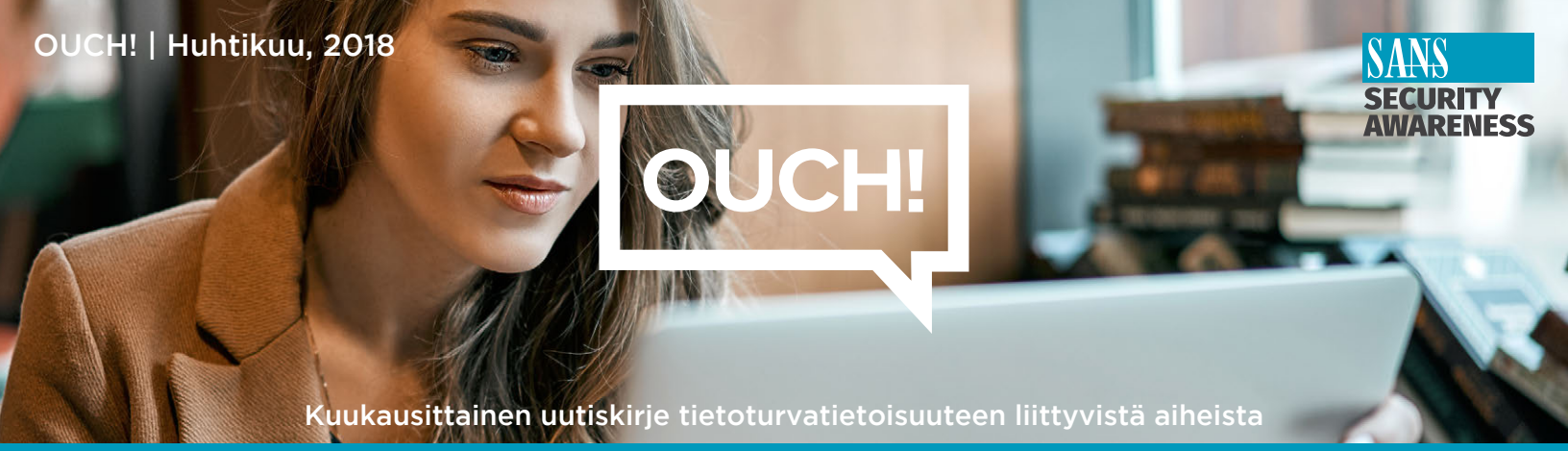

Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

Pysäytä kalastelu!

Yleiskatsaus

Sähköposti ja muut viestintäpalvelut (kuten Skype, Twitter ja Snapchat) ovat nykyisin pääasiallisia kommunikointivälineitämme, joita käytämme päivittäiseen työskentelyyn, sekä tuttujen ja perheen kanssa kommunikoimiseen. Koska niin monet ihmiset ovat riippuvaisia näistä palveluista, ovat ne myös suuressa roolissa, kun haitalliset tahot suunnittelevat hyökkäyksiään. Erinäisistä hyökkäyksistä suosituin tyyppi tässä yhteydessä on kalastelu. Tässä uutiskirjeessä opit mitä kalastelu on ja miten voit havaita ja pysäyttää kalasteluhyökkäykset, töissä tai vapaa-ajalla.

Mitä kalastelu on

Kalastelulla tarkoitetaan hyökkäystä jossa haitallinen taho käyttää sähköpostia, viestintäsovellusta tai sosiaalista mediaa saadakseen käyttäjän tekemään tiettyjä asioita, esim. klikkaamaan tiettyä linkkiä, luovuttamaan salasanan tai avaamaan liitetiedoston. Hyökkäyksiä tekevät tahot tekevät paljon töitä saadakseen kalasteluviestit näyttämään mahdollisimman luotettavilta ja käyttävät hyväkseen ihmisten luonnollisia ominaisuuksia, kuten kiireellisyyden tunnetta tai uteliaisuutta. Viestit näyttävät usein siltä, että ne ovat tulleet joltakin jonka tunnet tai tiedät, esim. ystävä tai luotettava yritys jonka palveluita usein käytät. Viesteissä käytetään usein aitoja logoja tai muita merkkejä jotka vahvistavat aitouden tunnetta. Hyökkäysviestejä lähetetään miljoonille ihmisille, koska hyökkääjät eivät tiedä kuka viestiin takertuu, mutta mitä useammalle viesti lähtee, sen suuremmaksi muuttuu todennäköisyys, että joku ottaa viestin tosissaan.

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.
- Painostus tekemään jotain mitä yrityksesi tietoturvaohjeistukset tai prosessit eivät salli
- Viestissä viitataan uteliaisuuteen tai viesti vaikuttaa liian hyvältä ollakseen totta (ei, et ole voittanut arvonnassa, varsinkaan jos et osallistunut)

- Nimesi sijaan viesti alkaa yleisellä lausahduksella, kuten arvoisa asiakas. Useimmat sinulle viestejä lähettävät tahot tietävät nimesi.
- Sähköpostissa pyydetään erittäin 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
- Viesti tulee oikeasta sähköpostista, mutta kun vastaat viestiin, niin osoite on eri, esimerkiksi @gmail.com-päätteinen.
- 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. Jos viesti vaikuttaa oudolta, epäilyttävältä tai on liian hyvä ollakseen totta, se saattaa olla kalasteluviesti ja yksinkertaisinta on vain poistaa se.

Uutiskirjeen kääntäjä Kirill Filatov (KTM) on GIAC-sertifioitu tietoturvaa rakastava, kokenut IT-ammattilainen. Kirill turvaa tällä hetkellä Nebula Oy:n asiakkaiden liiketoimintaa konsultoimalla ja kehittämällä asiakkaiden tietoturvaviitekehyksiä ja toimintamalleja.

Vierastoimittaja

Tonia Dudley on kehittänyt ja vastannut tietoturvatietoisuuohjelmista vuodesta 2011 asti ja hänen saavutuksiinsa kuuluu mm. palkintoja voittanut kalastelunesto-ohjelma. Löydät Tonian www.linkedin.com/in/toniadudley.

Lähteet

Sosiaalinen hakkerointi:	https://www.sans.org/u/Cb1
Auta muita suojaamaan itsensä:	https://www.sans.org/u/Cb6
Parhaat vinkin turvalliseen sähköpostin käyttöön:	https://www.sans.org/u/Cbg
Toimitusjohtajahuijaus:	https://www.sans.org/u/Cbl
OUCH! Käännökset ja arkistot:	https://www.sans.org/u/Cbq

Lisenssi