SANS SECURITY AWARENESS

OUCH! | Marraskuu 2017

Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

- **Väärennetyt verkkokaupat**
- **Laitteesi**
- **Luottokorttisi**

Turvallisuus verkkokaupoissa

Yleisesti

Tuleva lomakausi lähestyy ja miljoonat ihmiset etsivät täydellisiä lahjoja. Monet valitsevat verkkokaupat välttääkseen ruuhkat ja löytääkseen parhaimmat hinnat. Valitettavasti lomakausi on myös verkkorikollisten lempiaika vuodesta ja siksi tämän kuun uutiskirjeessä keskitymme turvalliseen verkkokauppakäymiseen ja tapoihin joilla voit suojata itsesi verkko-ostoksilla.

Vierastoimittaja

Lenny Zeltser rakentaa tietoturvatuotteita Minerva Labs-nimisessä yrityksessä ja opettaa haittaohjelmilta suojautumistae SANS Instituutissa. Lenny on aktiivinen Twitterissä **@lennyzeltser** ja kirjoittaa turvallisuusaiheista blogia osoitteessa **zeltser.com**.

Väärennetyt verkkokaupat

Vaikka suurin osa verkkokaupoista on täysin asiallisia ja turvallisia, verkossa on valitettavasti myös sellaisia jotka eivät ole. Rikolliset luovat väärennettyjä verkkokauppoja, joissa on kopioitu jonkun tunnetun verkkokaupan komponentteja, ulkonäköä tai brändejä. Kun etsit verkosta parhaita tarjouksia, hakukoneet saattavat ohjata sinut tällaiselle väärennetylle sivustolle. Kun valitset itsellesi sopivaa verkkokauppaa, suhtaudu skeptisesti poikkeuksellisen halpoja hintoja tai muualta loppuneita tuotteita tarjoaviin kauppoihin. Tallaisessa tapauksessa on hyvin todennäköistä, että et tule koskaan saamaan tilaamiasi tuotteita tai tilaamasi tuotteet saattavat olla väärennettyjä tai laittomasti hankittuja. Voit suojata itseäsi seuraavin keinoin:

- Jos mahdollista, niin asioi verkkokaupoissa joista sinulla on kokemuksia tai joissa olet asioinut jo aiemmin.
- Varmista, että käyttämäsi kaupan verkko-osoite on asianmukainen ja sivuilta löytyy yrityksen fyysiset yhteystiedot. Jos sivu vaikuttaa epäilyttävältä, soita yritykseen ja varmista kaupan asianmukaisuus. Jos et löydä yhteystietoja tai saa ketään kiinni, kannattaa kyseisessä kaupassa jättää asioimatta.
- Kiinnitä huomiota varoitusmerkkeihin, kuten liian hyviin tarjouksiin, huonoon kirjoitusasuun tai kirjoitusvirheisiin
- Suhtaudu erittäin skeptisesti verkkosivuun joka näyttää tunnetulta verkkokaupalta, mutta osoite tai sen osa on erilainen kuin mihin olet tottunut. Jos olet esim. tottunut asioimaan www.amazon.com-kaupassa ja kaupan osoite www.store-amazon.com.
- Kirjoita käyttämäsi verkkokaupan nimi johonkin hakukoneeseen ja kirjoita nimen perään sanoja kuten huijaus,

Turvallisuus verkkokaupoissa

älä asioi täällä, huono tms. ja yritä löytää muiden ihmisten kokemuksia kyseisestä kaupasta. Arvostelujen puute on myös aihe huolestumiseen.

- Ennen ostamista, varmista että yhteys verkkokauppaan on kryptattu. Verkkosivun osoitteen pitäisi alkaa https:// tai verkkoselaimen pitäisi näyttää vihreän lukon kuvaan osoitepalkissa.

Muista aina, että vaikka kauppa näyttää asianmukaiselta, se ei välttämättä sitä ole. Jos sinua huolestuttaa joku, niin tutki asiaa tarkemmin. Jos et ole täysin varma kaupan asianmukaisuudesta, älä käytä sitä. Etsi mieluummin kauppa jossa olet aikaisemmin turvallisesti asioinut ja osta sieltä. Et välttämättä löydä yhtä halvinta hintaa, mutta ostokokemuksesi menee hyvin ja turvallisesti.

Suojaa itsesi verkko-ostoksilla käyttämällä vain luotettavia ja turvallisia verkkokauppoja.

Laitteesi

Asiallisen verkkokaupan valinnan lisäksi on tärkeää varmistaa, että käyttämäsi laitteet ovat asianmukaisesti suojattu. Kyberrikolliset yrittävät infektoida koneesi haittaohjelmilla saadakseen koneeltasi tietojasi, kuten salasanoja tai luottokorttitietoja. Voit suojata laitteesi seuraavilla tavoilla:

- Jos taloudessasi on lapsia, suosittelemme erillisen laitteen hankkimisesta lasten käyttöön. Lapset ovat uteliaita käyttäessään teknologiaa ja tämän vuoksi suuremmassa vaarassa laitteiden saastumisen osalta. Erillistä laitetta käytettäessä vähennät haittaohjelmatartunnnan riskiä. Asenna aina kaikki laitteiden päivitykset ja käytä tietoturvasovelluksia kaikilla laitteilla. Tämä hankaloittaa kyberrikollisten toimia merkittävästi.
- Yhdistä laitteesi vain tunnettuihin verkkoihin, kuten kotiverkkoosi. Julkisten verkkojen käyttäminen uutisten lukemiseen tai kevyeen surffailuun voi harkinnanvaraisesti olla ok, mutta kaupankäyntiin tai verkkopankin käyttöön ei näitä ole suositeltavaa käyttää.

Luottokorttisi

Tarkkaile luottokorttitapahtumiasi vähintään kuukausittain huomataksesi mahdolliset epäilyttävät tapahtumat. Monet pankit tarjoavat erinäisiä rajoituksia ja valvovia työkaluja luottokorttien käyttöön, näihin kannattaa perehtyä verkkopankkisi

Turvallisuus verkkokaupoissa

turvallisuusosioissa tai voit kysyä pankiltasi mitä vaihtoehtoja he tarjoavat tiliesi suojaamiseen. Toinen vaihtoehto on käyttää erillistä luottokorttia verkko-ostoksiin, jolloin huomaat mahdolliset asiattomat tapahtumat helpommin ja nopeammin, ja voit helposti sulkea kortin tarvittaessa vaikuttamatta muihin kortteihisi. Jos epäilet, että korttiasi on käytetty väärin, ota välittömästi yhteys pankkisi ja kerro heille tapahtuneesta. On myös suositeltavaa käyttää verkkokaupoissa korttisi credit-ominaisuutta, debit-ominaisuuden sijaan, koska mahdollisessa väärinkäyttötapauksessa rahojen palauttaminen voi olla helpompaa. Nykyisin on myös tarjolla maksutapoja, joissa maksu tapahtuu niin, että luottokorttisi tiedot eivät paljastu kauppiaalle ollenkaan, voit esim. käyttää PayPalia tai vastaavia toimijoita, ota tällöinkin huomioon näiden palveluiden tietoturva ja luotettavuus.

LUE LISÄÄ

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

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.

Lähteet

Sosiaalinen hakkerointi:	https://securingthehuman.sans.org/ouch/2017#january2017
Neljä askelta turvallisuuteen:	https://securingthehuman.sans.org/ouch/2016#october2016
Kotiverkkosi suojaaminen:	https://securingthehuman.sans.org/ouch/2016#february2016
SANS, Päivän tietoturvavinkki:	https://www.sans.org/tip_of_the_day.php

Lisenssi