Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

Verkkopelaamisen turvallisuus

Esittely

Verkkopelaaminen on loistava tapa pitää hauskaa, mutta se sisältää merkittävän määrän uniikkeja riskejä. Tässä uutiskirjeessä kerromme mitä voit tehdä suojataksesi itseäsi ja perhettäsi verkkopelien maailmassa.

Vierastoimittaja

Jake Williams on Rendition Infosec yrityksen perustaja ja pääkonsultti. Jake on sertifioitu SANS-kouluttaja ja osallistunut monien SANS-kurssimateriaalien kirjoittamiseen. Hänet löytää Twitteristä **@MalwareJake** ja hän myös bloggaa aktiivisesti osoitteessa **malwarejake.blogspot.com**.

Itsesi suojaaminen

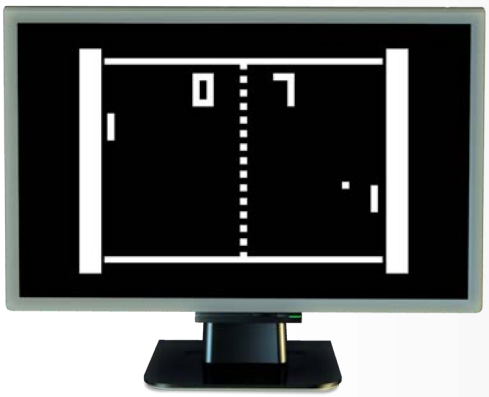
Verkkopelaamisesta tekee erityisen hienoa se, että voit pelata ja kommunikoida ympäri maailmaa pelaavien pelaajien kanssa. Usein pelaaja ei edes tiedä kenen kanssa tosiasiassa pelaa. Vaikka suurin osa verkkopelaajista pelaa pelejä pitääkseen hauskaa, joukkoon mahtuu valitettavasti aina ihmisiä, jotka haluavat aiheuttaa jonkinlaista vahinkoa. Tässä joitakin asioita mitä voit ottaa huomioon suojataksesi itseäsi.

- Noudata varovaisuutta saadessasi viestin, joka edellyttää sinua tekemään jotain, kuten klikkaamaan linkkiä tai lataamaan tiedostoja. Aivan kuten kalasteluhyökkäyksissä, “pahikset” yrittävät huijata sinua tekemään jotain, mikä todennäköisesti saastuttaa koneesi. Jos viesti vaikuttaa oudolta, kiireelliseltä tai on liian hyvää ollakseen totta, ole varuillasi sillä kyseessä voi olla jonkinlainen hyökkäys.
- Monissa verkkopeleissä on omat taloudelliset markkinat, joissa voi käydä kauppaa, vaihtaa tai ostaa virtuaalista omaisuutta. Aivan kuten oikeassakin maailmassa, virtuaalisessakin maailmassa on huijareita, jotka yrittävät huijata sinua tai jopa varastaa virtuaalista omaisuuttasi.
- Ole huolellinen, kun käyt verkossa kauppaa omaisuudesta, jossa käytetään oikeaa rahaa. Käytä oikeaa rahaa vain kaupoissa, jotka on yleisesti tunnistettu turvalliseksi.
- Rajoita omaa tai lastesi verkossa jakamaa tietoa. Älä koskaan jaa henkilökohtaista tietoa, kuten salasanoja tai kotiosoitteita.
- Monet verkkosivut, kuten verkkopankit, käyttävät turvallisuuskysymyksiä identiteetin varmistamiseen. Hyökkääjät ovat joissakin tilanteissa käyttäneet näiden kysymysten vastauksia huijatessaan tai lähettäessään kaveripyyntöjä verkkopeleissä. Muista, että sinulla ei ole velvollisuutta vastata mihinkään kysymyksiin, mitä sinulta verkkopelien yhteydessä kysytään.

Verkkopelaamisen turvallisuus

Tietokoneen ja tilien suojaaminen

Seuraava vaihe on verkkopeleihin käytettävien välineiden suojaaminen. Koska vihamieliset tahot yrittävät ottaa konettasi tai tilejäsi haltuunsa, sinun pitää suojautua.



Tärkeintä turvallisessa verkkopelaamisessa on vahvojen salasanojen käyttö, päätelaitteen suojaaminen ja terveen järjen käyttäminen vieraiden henkilöiden kanssa kommunikoidessa tai pyyntöjä saadessa.

- Käytä vahvaa salasanaa työasemallesi ja kaikissa pelitileissä. Tällä tavalla vaikeutat hyökkääjien toimia. Jos peli tarjoaa mahdollisuuden kaksivaiheselle tunnistautumiselle, käytä myös sitä. Varmista myös, että käytät pelitileilläsi eri salasanoja kuin muualla, tällä tavalla vaikka salasanasi saadaan haltuun, muut tilit pysyvät turvassa.
- Suojaa työasemasi käyttämällä aina viimeisintä versiota käyttöjärjestelmästä ja verkkopelistä. Aivan kuten käyttöjärjestelmissä ja verkkoselaimissa, myös peleissä on tunnistettu haavoittuvuuksia, joita hyökkääjät voivat käyttää hyväkseen ja hakkeroitua tilillesi tai työasemallesi. Käyttämällä uusimpia versioita, eliminoit suurimman osan tunnetuista haavoittuvuuksista.
- Käytä virustorjuntasovellusta, ja varmista että käytössäsi on uusin versio ja että tarkistus tapahtuu reaaliajassa.
- Lataa pelejä vain tunnetuista lähteistä. Jos olet asentamassa peliä, varmista että se on ladattu pelitoimittajan sivulta tai jostakin muusta luotetusta lähteestä. Hyökkääjät luovat usein väärennettyjä tai infektoituneita versioita pelistä ja jakavat näitä omilta palvelimiltaan. Jos asennat tälläisen version, vihamielinen taho saattaaa saada koko työasemasi hallintaansa.
- Pelien lisäpaketteja, joita myös peliyhteisöt saattavat kehittää, käytetään usein uusien ominaisuuksien lisäämiseen peleihin. Hyökkääjät saattavat saastuttaa näitä haittaohjelmilla, joita virustorjuntatuotteiden voi olla vaikeaa havaita. Aivan kuten pelien lataamisen osalta, varmista myös että lataat lisäominaisuudet vain luotettavista lähteistä. Jos lisäominaisuudet vaativat virustorjuntaohjelmiston tai palomuurin muokkaamista tai poistamista, älä käytä niitä.
- Verkosta löytyy isot markkinat erinäisille huijausohjelmille, joiden avulla peleissä pystyy huijaamaan ja menestymään paremmin. Sen lisäksi, että näiden käyttö on epäeettistä, monet huijausohjelmat ovat itsessään niin sanottuja rootkittejä, eli käytännössä tehokkaimpia haittaohjelmia. Älä koskaan asenna minkäänlaisia huijausohjelmia.
- Käy tarkkaan läpi pelaamasi verkkopelin valmistajan internetsivu. Monet pelisivut sisältävät tietoa miten voit suojata järjestelmäsi ja itsesi hyökkäyksiltä, noudata myös näitä ohjeita.
- Lisäksi, noudata samoja ohjeita pelatessasi mobiililaitteella. Kyberrikolliset ovat alkaneet kehittää hyökkäystapoja myös mobiililaitteita kohtaan.

Verkkopelaamisen turvallisuus

Vanhemmille

Jos sinulla on lapsia, varmista että he seuraavat yllämainittuja ohjeita (mielellään avusta heitä varmistamaan). Lisäksi keskustele lastesi kanssa verkkopelaamiseen liittyvistä riskeistä. Valistus ja avoin keskustelu lasten kanssa on tehokkain tapa heidän suojamisekseen. Yksi hyvä tapa saada lapset puhumaan pelaamisesta on osoittaa kiinnostusta ja pyytää heitä näyttämään miltä peli näyttää ja mitä kaikkea pelimaailmasta löytyy. Lisäksi voit pyytää heitä kuvailemaan minkälaisia henkilöitä he verkkomaailmassa tapaavat. Parhaimmassa tapauksessa voit jopa pelata peliä heidän kanssaan. Verkkopelit ovat nykyisin hyvin monelle lapselle ja nuorelle erittäin iso osa sosiaalista elämää. Keskustelemalla ja kuuntelemalla heitä voit huomata ongelmia ja suojella heitä tehokkaammin kuin monella teknologiaan pohjautuvalla ratkaisulla.

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.

Lähteitä

Käyttäjän manipulointi:	http://www.securingthehuman.org/ouch/2014#november2014
Kalasteluhyökkäykset:	http://www.securingthehuman.org/ouch/2013#february2013
Salasanat:	http://www.securingthehuman.org/ouch/2013#october2013
Mikä on Anti-Virus?:	http://www.securingthehuman.org/ouch/2014#december2014
Turvallisesti verkossa:	http://www.staysafeonline.org/stay-safe-online/for-parents/gaming-tips

Lisenssi

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