TIETOSUOJAVALTUUTETUN TOIMISTO

PHARMING, MITÄ SE ON?

Päivitetty 27.07.2010

www.tietosuoja.fi

MITÄ ON PHARMING?

KUINKA TIETOKONEYHTEYTESI VOIDAAN KAAPATA JA IDENTITEETTISI VARASTAA

Olet ostamassa kirjoja verkkokaupasta ja päädyt tunnetun kaupan sivustolle, jossa pyydetään maksamista varten tunnuksiasi. Näin ostaminen ja maksaminen on vaivatonta ja turvallista – vai onko? Kirjojen tulo viivästyy, pian paljastuu myös, että tilitietojasi on käytetty väärin, tililtäsi on siirretty rahaa muille tileille. Selviää, että hakkeri on kaapannut tietokoneesi, ohjannut sinut omalle huijaussivustolleen, siepannut salassa pidettäviä tunnuksiasi ja käyttänyt niiden avulla tiliäsi. Olet joutunut tietokoneesi ja tietoliikenneyhteyksiesi kaappauksen, pharmingin uhriksi. Uhriksi voi joutua jokainen, joka käyttää internetiä ja verkkopalveluja.

Mitä pharming on?

Hakkeri yrittää luvattomasti saada käyttäjän tietokoneen hallintaansa ja ohjata käyttäjä asiallisilta palvelimilta ja sivustoilta hakkerin omille palvelimille ja sivustoille. Tätä varten hakkeri ujuttaa käyttäjän tietokoneelle vakoiluohjelman, jonka avulla hän saa tietokoneen haltuunsa, seuraa käyttäjän tietoverkon ja verkkopalvelujen käyttöä sekä ohjaa käyttäjän tietoliikennettä ja palvelujen käyttöä omille sivustoilleen. Tämä voi tapahtua ilman että käyttäjä myötävaikuttaa siihen mitenkään tai edes huomaa mitään.

Hakkerin tarkoituksena on saada käyttäjä luovuttamaan salassa pidettäviä tunnuksia ja muita tietoja, joiden avulla hän voi hyödyntää käyttäjän pankkitilejä ja saada muita etuuksia itselleen. *Phishingissä huijari suostuttelee käyttäjää avoimesti antamaan salassa pidettäviä tietoja, pharmingissa huijari yrittää saada käyttäjältä tietoja tämän tietämättä tästä mitään.*

Mitä seurauksia pharmingista voi olla?

Arkaluonteiset ja salassa pidettävät tietosi voivat paljastua ja jos näitä päätyy julkisuuteen, sinulle voi aiheutua ongelmia, esimerkiksi maineen menetyksiä. Identiteettisi voidaan varastaa, sitä voidaan käyttää väärin siten, että menetät rahaa tai muita etuuksia. Identiteettisi ja muiden tietojesi väärinkäytöstä aiheutuu yleensä paljon vaivaa, kun korjaat vahinkoja, vaihdat tunnuksiasi ja oikaiset virheitä. Voit olla tahtomattasi ja tietämättäsi osallisena vahingollisessa tai pahimmillaan rikollisessa toiminnassa, jos tietokonettasi käytetään esimerkiksi roskapostien välittämiseen, palvelujen estämiseen tai laittomaan rahan keruuseen.

Mitä oikeuksia Sinulla on?

Sinulla on tietenkin oikeus torjua tunkeutumiset tietokoneellesi, tietokoneellesi ei saa asentaa tietämättäsi ohjelmia ja tiedostoja. Ulkopuoliset eivät saa seurata tietokoneesi toimintaa, ellei se liity tietokoneen toiminnan ja turvallisuuden varmistamiseen. Sinun tulee olla tietoinen tästä ylläpidosta ja sinulla tulee olla mahdollisuus vaikuttaa tähän. Tietokoneen käyttöäsi ei saa ilman suostumustasi tai ilman laillista perustetta kukaan ulkopuolinen seurata.

Mikäli tietojasi on luvatta anastettu ja käytetty, sinulla on tietenkin oikeus yrittää selvittää, kuka on anastanut tietojasi ja mihin niitä on käytetty. Lisäksi sinulla on oikeus saattaa tietosi ajan ta-

salle, mikäli ne ovat muuttuneet tai tuhoutuneet. Sinulla on oikeus saada pharmingin avulla saadut tiedot hävitetyksi. Mikäli tietojesi väärinkäytöstä aiheutuu sinulle vahinkoa, sinulla voi olla oikeus saada korvaus vahingosta.

MITÄ VOIT TEHDÄ?

1) Pidä tietokoneesi turvallisena

- suojaa tietokoneesi ulkopuolisia tunkeutujia vastaan, pidä palomuurisi ja virustorjuntasi ajan tasalla
- käytä turvallisia tietokoneen ja tietoverkon käytön välineitä ja ohjelmia, salaa arkaluonteisten ja salassa pidettävien tietojesi siirtäminen verkossa

2) Vähennä altistumista huijauksille

- käytä suojausohjelmia, ne paljastavat väärennettyjä web-osoitteita, käytä myös suodatusohjelmia estämään ns. ponnahdusikkunoita, joita käytetään pharming-huijauksissa
- jos on mahdollista, käytä anonyymiä verkkoidentiteettiä
- tarkista, että käyttämäsi sivusto ja yhteys ovat turvallisia, ota huomioon, että myös huijari voi käyttää turvalliselta näyttäviä sivustoja ja yhteyksiä
- pyri varmistumaan käyttämäsi sivuston aitoudesta, ota huomioon, että myös huijari voi muuttaa myös osoitteitaan ja linkkejään näyttämään aidoilta
- jos tarvitset yhteyttä palvelun tarjoajaasi, esimerkiksi pankkiin, varmistu, että olet oikean pankin sivustolla ja/tai käytä puhelinnumeroa, jonka oikeellisuuden olet varmistanut
- älä käy turhaan tuntemattomilla sivustoilla
- älä vastaile epämääräisiin yhteydenottoihin äläkä usko epämääräisiä lupauksia
- älä klikkaa linkkiä sähköpostiviestissä, jossa pyydetään salassa pidettäviä henkilötietojasi
- älä luovuta henkilökohtaisia tietojasi verkossa, ellet ole varmistanut tietojen kysyjän asiallisuutta

3) Hanki valmiudet huijauksen estämiseksi

- opi estämään asiattomien pääsy tietokoneeseesi
- opi liikkumaan ja käyttämään palveluja verkossa turvallisesti
- opi tuntemaan turvalliset verkkopalvelut
- opi tunnistamaan huijausyritykset

4) Raportoi havaitsemistasi asiattomuuksista

- jos epäilet joutuneesi pharming-kaappauksen uhriksi, raportoi sivuston ylläpitäjiä, joiden verkkopalveluja on käytetty väärin
- mikäli henkilötietojasi on käsitelty asiattomasti, ota yhteys käsittelijään, voit ottaa yhteyden myös tietosuojaviranomaisiin
- mikäli olet joutunut huijauksen uhriksi ja menettänyt esimerkiksi rahaa, ota yhteys poliisiin

Kts. myös tietosuojavaltuutetun toimiston esitteet osoitteessa www.tietosuoja.fi:

Identiteettivarkaus mikä se on?
Huijaussähköposti mikä se on?
Palomuuri mikä se on?
Tietokoneen kaappaus mikä se on?