TIETOSUOJAVALTUUTETUN TOIMISTO

HUIJAUSSÄHKÖPOSTI, MIKÄ SE ON?

Päivitetty 15.09.2010

www.tietosuoja.fi

MIKÄ ON HUIJAUSSÄHKÖPOSTI?

SINULLE ON SÄHKÖPOSTIA HUIJARILTA!
- mitä on phishing?

Olet saanut pankiltasi sähköpostiviestin, sen mukaan pankkitunnuksiasi on yritetty käyttää väärin. Pankki pyytää sinua vaihtamaan tunnuksesi turvallisemmaksi, samalla se pyytää ilmoittamaan uuden tunnuksen lisäksi nykyisen tunnuksen sekä seuraavat viisi kertakäyttösalasanaa, jotta pankin turvallisuusyksikkö voi testata ja arvioida uuden tunnuksen turvallisuuden. Hyvä, että valvovat tilien turvallisuutta ja ilmoittavat nopeasti sähköpostilla. Pankki pyytää tietoja viestissä olevan linkin kautta. Klikkaat linkkiä, sieltä avautuvat tutut pankin verkkosivut.

Parin viikon päästä saat taas pankilta ilmoituksen, nyt tiliesi mahdollisista väärinkäytöistä ja nyt kirjeellä. Käy ilmi, että olet saanut joltakin huijarilta viestin, käynyt tämän rakentamalla huijaussivulla ja luovuttanut tälle pankkitunnuksesi, näitä hyväksikäyttäen tiliäsi on käytetty viime päivien aikana. Olet joutunut tietojesi luvattoman kalastelun (phishing) uhriksi.

Miten voidaan tietoja huijata Internetissä?

Internetin ja sen palvelujen käyttäjiä on mahdollista huijata lukemattomin tavoin. Joku voi esiintyä jonain toisena ja lähettää sinulle viestejä tämän nimissä sekä pyytää sinua lähettämään luottamuksellisia ja salassa pidettäviä tietoja itselleen. Huijauksen lavastamiseksi on rakennettu esimerkiksi pankin verkkosivustoa muistuttava sivusto ja pyytää sen avulla sinulta pankkitunnuksiasi. Huijausyritykset ja –sivustot ovat yhä taidokkaampia. Pankkitietojesi pyydystelyn ohella kalastelija voi esiintyä organisaation tietojenkäsittelystä vastaavana yksikkönä, joka pyytää käyttäjätunnuksiasi ja salasanojasi, joiden avulla pääset eri tietojärjestelmiin ja palveluihin verkossa. Tämän kaltainen huijaus on lähes aina rikos.

Sinulle voi koitua suurta vahinkoa, mikäli huijari onnistuu kalastelemaan sinulta salassa pidettäviä tietoja ja käyttämään niitä tarkoituksiinsa. Voit menettää rahaa, joku toinen käyttää sinulle kuuluvia oikeuksia ja etuuksia, mutta ennen kaikkea voit menettää luotettavuutesi. Voit joutua rekisteröidyksi väärin perustein esimerkiksi maksuhäiriörekistereihin, joiden tietojen perusteella tehdään lukuisia sinua koskevia päätöksiä. Pahimmassa tapauksessa voit joutua jopa rikosrekisteriin. Ehkä työläintä ja aikaa vievintä on virheellisten tietojen oikaiseminen, ethän edes tiedä, mihin kaikkiin rekistereihin virheelliset tietosi ovat siirtyneet.

Tietojen tietoverkossa huijaamisen välttäminen ei ole vaikeaa, kunhan omaksut muutamia viisaita käytäntöjä. Jotta pystyt välttämään tietojesi sieppaamisen, sinun täytyy tunnistaa huijarin tavat toimia. Lisäksi sinun on hyvä tuntea esimerkiksi pankkien tai tietojenkäsittelystä vastaavien yksikköjen tavat toimia, kun ne ilmoittavat epäselvyyksistä. Sinun on myös syytä etukäteen miettiä, miten toimit, mikäli epäilet joutuneeksi huijauksen uhriksi.

TOIMI VIISAASTI JA NOPEASTI

Tässä esitetään muutamia ohjeita siitä, miten vähennät huijaukseksi joutumisen mahdollisuuksia, miten paljastat mahdollisia huijausyrityksiä ja miten toimit, jos epäilet joutuneesi huijausyrityksen kohteeksi:

1) Ota selvää, miten tietoverkossa palveluja tarjoavat tahot toimivat

- ota selvää, miten palveluja sinulle tarjoavat tahot, esimerkiksi pankit toimivat, miten ne turvaavat palvelusivuston turvallisuuden, käyttävätkö ne esimerkiksi salausta yhteydenpidossa, luotettava palveluntarjoaja kertoo näistä sivuillaan
- ota selvää, miten palveluntarjoajasi ovat yhteydessä sinuun esimerkiksi kun muutetaan tunnuksia ja vastaavia; sähköpostitse kukaan luotettava taho ei pyydä eikä lähetä salassa pidettäviä tietoja
- ota selvää, miten ne yleisesti käsittelevät tietojasi, tämän saat parhaiten selville tutustumalla niiden tietosuojaperiaatteisiin ja –politiikkaan; luotettava palveluntarjoaja kertoo niistä sivuillaan, toki huijarikin voi esitellä käytäntöjään luotettavan oloisesti

2) Noudata itse turvallisia ja luotettavia sähköpostin ja muun verkon käytön periaatteita

- sähköpostin lähettäjätietoja on helppo väärentää; älä vastaa tuntemattomiin ja epäluotettavilta vaikuttaviin viesteihin
- älä lähetä salassa pidettäviä tietojasi sähköpostitse, ellet ole suojannut lähetystä esimerkiksi salaamalla tiedot, verkossa ei ole syytä yleensäkään paljastaa arkaluonteisia tietoja itsestään, ellei ole varmistunut toisen osapuolen luotettavuudesta
- pyri varmistumaan sähköpostia lähettävän tahon aitoudesta, samoin pyri varmistumaan verkkopalveluja tarjoavan tahon sivuston aitoudesta

3) Toimi nopeasti, jos epäilet joutuneesi huijauksen tai sen yrityksen kohteeksi

- ota esimerkiksi sähköpostiviestin lähettäjäksi esitetyltä taholta suoraan selvää, mistä on kyse
- mikäli epäilet joutuneesi huijauksen tai sen yrityksen kohteeksi, ilmoita niille tahoille, esimerkiksi pankeillesi, joita ehkä käytetään huijauksessa
- sulje mahdollisen väärinkäytön kohteiksi joutuneet tai joutuvat tilit
- vaihda huijareille mahdollisesti paljastuneet tunnuksesi ja salasanasi
- mikäli kyseessä on ilmeinen rikos, ota yhteys poliisiin
- mikäli henkilötietojasi on käytetty väärin, ota myös yhteys poliisiin
- mikäli henkilötietojesi käsittelyssä ja käytössä on epäselvyyksiä, ota yhteys kyseiseen käsittelijään, voit ottaa yhteyden myös tietosuojaviranomaisiin