Tietojen kalastelu

Tietojen kalastelu (phishing) on taloudellisesti hyödynnettävän tiedon, kuten verkkopankkitunnusten, luottokorttinumeroiden tai henkilötietojen laitonta hankkimista. Henkilökohtaisia tai seurakunnan tietoja voidaan urkkia tekaistujen sähköpostiviestien tai verkkopalveluiden välityksellä.

Sähköpostitse saattaa tulla aidolta vaikuttava kysely, jossa vastaanottajaa pyydetään ilmoittamaan verkkopalvelun toiminnan varmistamiseksi käyttäjätunnuksia, salasanoja tai muita henkilökohtaisia tietoja. Käyttäjää voidaan myös houkutella sähköpostiviestillä siirtymään www-sivustolle, jossa pyydetään luovuttamaan tietoja. Sivusto voi olla ulkoisesti esimerkiksi rahoituslaitoksen sivujen näköiset. Todellisuudessa nämä sivustot ovat hyökkääjän luomia huijaussivustoja, jonne syötetyt tiedot päätyvät hyökkääjän käsiin.

Ns. nigerialaiskirjeillä luvataan runsaasti rahaa, jos vain teet itse aluksi "nimellisen" rahasiirron viestin lähettäjän tilille vaikkapa rahan siirtämistä tai veroja varten. Luvattuja suuria rahoja on turha odottaa. Uhreja lähestytään yleensä sähköpostilla, toisinaan myös faksilla tai postitse.

- ✓ Luotettavaa liiketoimintaa harjoittavat yritykset, kuten esim. pankit, eivät pyydä lähettämään tai päivittämään tietoja sähköpostitse. Näihin viesteihin ei pidä vastata eikä niissä olevia linkkejä pidä klikata.
- ✓ Älä luota sähköpostissa olevaan lähettäjätietokentän sisältöön. Sähköpostin lähettäjätietokenttä voidaan helposti väärentää vaikkapa muotoon asiakaspalvelu@omapankkisi.fi.
- ✓ Älä luota, että sähköpostissa tai www-sivustolla olevat linkit johtavat sinne, mitä linkeissä lukee.
- ✓ Turvallisin tapa siirtyä sähköisen asiointipalvelun sivustolle on kirjoittaa itse asiointipalvelun www-sivun osoite selaimen osoiteriville tai käyttää selaimeen itse tekemäänsä pikalinkkiä (Suosikit tms.).
- ✓ Tarkista aina ennen luottamuksellisten tietojen syöttämistä, että olet oikean organisaation sivustolla, ja että sivustolla käytettään SSL-suojausta. Verkkopankissa osoiterivillä olevassa osoitteessa pitää näkyä pankin domain-nimi. Sivustolla käytetään SSL-suojausta, jos selaimessa näkyvä lukko on kiinni ja osoiterivillä oleva osoite alkaa https-tekstillä.