Käytä konetta oikein

Marko Kivelä
Tietotekniikkaosasto

Viime vuosina on tekniseen tietoturvaan kiinnitetty paljon huomiota. Koneiden turvallisuutta on lisätty niin tietoturvapäivityksillä, palomuureilla kuin yhä monipuolisemmilla haittaohjelmia torjuvilla sovelluksilla. Tärkein tietoturvaongelma ei ole kuitenkaan koskaan ollut itse laitteessa, vaan koneen ja tuolin välissä. Parhaatkaan turvaohjelmat eivät auta, jos koneen käyttäjä itse toimii varomattomalla tavalla.

Virheellisiä toimintatapoja on useita, mutta jo muutamalla pikku toimenpiteellä voidaan helposti vähentää turhia riskejä. Muistutettakoon vielä, mistä mahdolliset hyökkääjät ovat kiinnostuneita, eli mitä pahantekijät tavoittelevat. Varsinkin virusten ja tiettyjen haittaohjelmien tavallisin tavoite on kaapata yksittäinen kone joko sillanpääasemaksi laajempaan murtoon tai esimerkiksi laittoman materiaalin jakeluun tai roskapostin levityskoneeksi.

Ihmisten herkkäuskoisuuteen perustuva *phishing* sekä monet vakoiluohjelmat pyrkivät varastamaan käyttäjältä jotain. Joissain tapauksissa varastetaan käyttäjätunnuksia myöhempää murtautumista varten, mutta yhä useammin tavoitteena ovat suorat taloudelliset varkaudet, etenkin käyttäen hyväksi varastettuja luottokorttitietoja.

Älä ole herkkäuskoinen

Mitä sitten pitäisi välttää? On tietysti helppo sanoa, että älä käytä luottokorttia verkossa, mutta se olisi hätävarjelun liioittelua, sillä Internet on monessa suhteessa hyvä ja kätevä kauppapaikka. Kannattaa muistaa se, että omalla toiminnalla voi verkossakin turvallisuutta lisätä huomattavasti. Tärkeää on esimerkiksi, ettei nettisurffailun aikana hyväksy koneeseen mitään ylimääräistä, mitä sivulta yritetään koneelle tarjota, tai ylipäätään mitään, josta ei oikein tiedä, mistä on oikeasti kyse. Tämä on nimittäin oiva tapa saada koneeseen vakoiluohjelmia. Kaikkein tärkeintä kuitenkin on, ettei käyttäjä vapaaehtoisesti anna tietojaan rikollisille. Tätä tapahtuu turhan usein.

Phishing on yksi muotitermeistä. Se tarkoittaa mahdollisimman vakuuttavien viestien lähettämistä käyttäjille verkkokaupan, pankin tai muun tahon nimissä. Usein näissä viesteissä kerrotaan, että turvallisuuden varmentamiseksi halutaan, että käyttäjä auttaa tarkistamaan tahoja koskevien tietojen oikeellisuuden viestiin linkitetystä osoitteesta. Käyttäjän napsauttaessa linkkiä hän pääsee aidon näköiselle sivulle, jossa kysellään kaikkea mahdollista, siinä sivussa myös luottokorttitietoja. Kun käyttäjä vastaa kysymyksiin ja poistuu sivulta, ovat tiedot rikollisilla, jotka joko itse käyttävät niitä tai myyvät tietoja eteenpäin.

Myös osa roskapostista toimii vastaavanlaisella tavalla. Roskapostittaja eli ”spammeri” saattaa esimerkiksi vastaanottaa rahat, muttei lähetä mitään vastineeksi, tai hän saattaa kerätä luottokorttitietoja myöhempään käyttöön.

Omat tiedot salassa

Omien tietojen salaaminen ei rajoitu nettikyselyihin. Aina, jos käyttäjältä kysellään salasanoja, on syytä valpastua, sillä normaalisti käyttäjätuki ei niitä tarvitse. Koneen paikallisen järjestelmävalvojan (*administrator*) salasanakin on sellainen, että sen saa antaa vain ihmiselle, jonka käyttäjä itse tai paikallinen tuki on itse kutsunut paikalle korjaamaan konetta. Ja tällöinkin salasana kerrotaan mielellään, vain jos henkilö todistaa henkilöllisyytensä. Koska tietokonejärjestelmien käyttöoikeus on henkilökohtainen, ei tunnuksia ja salasanoja pidä myöskään jaella tutuille tai edes perheenjäsenille.