Netikäs

3. Tietoturva

Mediasivistysmateriaali osa 3/6

Turvallinen matka nettiin

Millainen on hyvä salasana?

Ritva, 67 vuotta:

“Virustorjunta hoituu perus-ohjelmillá.

Mediasivistys - turvallinen matka nettiin

Kyseleekö tietokoneesi päivityksistä? Oletko lukenut tietomurroista? Miten suojaat tietokoneesi viruksilta? Miksi pankki kyselee sähköpostissa verkkopankkitunnuksia? Onko salasanasi oma nimesi? Oletko saanut tuntemattomilta henkilöiltä yhteydenottoja, jossa sinulle luvataan lottovoiton verran rahaa?

Tietokoneen ja internetin käytöstä on hyötyä ja hupia monella tavalla. Muutama asia on kuitenkin hyvä ottaa huomioon, jotta nettisurffaaminen ja sähköinen asiointi olisivat mahdollisimman turvallisia. Tässä vihkosessa käsitellään tietoturvaa.

Mediasivistysmateriaali on osa Eläkeliitto ry:n ja EHYT ry:n yhteisen LähiVerkko-projektin materiaalituotantoa. Materiaali on tehty yhteistyössä seuraavien toimijoiden kanssa: Vanhustyön keskusliitto (VTKL) SeniorSurf, SenioriVerkko-hanke, ENTER ry, Seniorien ATK-yhdistys Savonetti ry, Joen Severi ry ja Mediakasvatusseura ry. Tämän materiaalin tekoon on saatu tukea RAY:lta. LähiVerkko-projekti kiittää mukana olleita muita tahoja ja ikäihmisiä, erityisesti Anna-Maija Muromaata kommentoinnista ja sisällönkehittämisestä.

Teksti: Jouni Ahonen
Oikoluku ja sisällöntarkistus: Eija Kalliala
Graafinen suunnittelu: Salla Vasenius.

Ilmestymisvuosi: 2015
www.netikas.fi

Mikä ihmeen tietoturva?

Tietoturva on laaja käsite, joka tarkoittaa mm. tietojen, laitteiden, järjestelmien ja tietoliikenteen suojaamista uhilta. Yleisimpiä uhkia ovat erilaiset huijausyritykset kuten pankkitunnusten kalastelu, henkilökohtaisen yksityisyyden loukkaukset, roskaposti, haittaohjelmat ja laitteiden rikkoutuminen.

Tietoturvasta huolehtiminen on tärkeää, vaikka omasta mielestäsi tietokoneellasi ei olisi mitään arvokasta. Jos tietokoneelle pääsee haittaohjelmia, niiden poistaminen on vaivalloista ja vie aikaa. Joskus tietokone joudutaan jopa asentamaan kokonaan uudestaan. Esimerkiksi roskapostittajat ovat kiinnostuneita tietokoneen hallinnasta, eivät niinkään sen sisältämistä tiedoista. Kaapatulla tietokoneella voidaan käyttäjän tietämättä lähettää suuret määrät sähköpostia, joka sisältää mainoksia tai haitallisia liitetiedostoja. Suomessakin on tapauksia, joissa huolimattomasti suojattu tietokone on päätynyt roskapostittajien hallintaan ja internet-operaattori on sulkenut liittymän vedoten roskapostitukseen. Pidäthän huolta tietoturvasta — autat itseäsi ja muita internetin käyttäjiä.

Tietoturva samaistetaan usein tietotekniikkaan ja ulkoisiin tietoturvauhkiin eli tahallisesti tehtyihin tietokoneviruksiin ja muihin haittaohjelmiin. Tietokoneviruksia ja haittaohjelmia vastaan on kehitetty erilaisia virustorjunta- ja tietoturvaohjelmia, jotka ovat lähes pakollisia useimmissa tietokoneissa. Niistä on olemassa sekä ilmaisia että maksullisia versioita. Käytännössä ne ovat yhtä turvallisia, mutta ilmaisversiot ovat usein englanninkielisiä ja ehkä hankalampia käyttää. Maksulliset tietoturvaohjelmistot maksavat yleensä muutaman euron kuukaudessa ja ostetaan vuodeksi kerrallaan. Jos koneesi on asianmukaisesti suojattu, tietoturvasi on siltä osin hyvällä mallilla.

Mikäli tietoturvaohjelmat ja tietokoneen muu ohjelmisto ovat ajan tasalla, pahin uhka tietoturvalle on yleensä käyttäjä itse. Internet on täynnä houkuttelevia tarjouksia, mainoksia ja arvontoja. Joillain sivuilla eteen saattaa aueta ilmoitus, jossa luvataan raha- tai tuotepalkintoja. Vastaavia mainoksia tulee myös lähes jokaiselle sähköpostin käyttäjälle. Yleensä ilmaisia tuotteita tai rahapalkintoja ei ole olemassa. Näillä huijausyrityksillä kerätään henkilötietoja tai yritetään saada hyväuskoinen käyttäjä lähettämään tekstiviesti maksulliseen numeroon. On hyvä pitää mielessä, että mikäli jokin asia internetissä kuulostaa liian hyvältä ollakseen totta, se tuskin on totta.

Julkisuudessa on usein ollut esillä phishing- eli tietojenkalasteluviestejä. Ikävimpänä muotona näistä ovat luottokortti- ja verkkopankkien tunnuslukujen kalastelu sähköpostiviesteillä, puhelimitse tai väärennetyillä verkkosivuilla. Yleensä huijauksissa käytetään poliisin, pankin tai perintäyhtiön nimeä. Uusia huijausyrityksiä varsinkin pankkien nimissä tapahtuu muutaman kerran vuodessa.

Näiltä huijausyrityksiltä on helppo suojautua pitämällä mielessä, että viranomaiset eivät koskaan kysy edellä mainittuja tunnuslukuja puhelimitse tai sähköpostitse. Kannattaa myös kiinnittää huomiota viestien oikeinkirjoitukseen. Huijausviestit on yleensä kirjoitettu huonolla suomen kielellä.

Esimerkki

Liisa avaa tietokoneen, kuten hänellä päivittäin on tapana. Tällä kertaa tutun aloitusnäytön sijaan ruudulle ilmestyy viesti:

POLIISI

Poliisihallituksen Keskusrikospoliisi Poliisin Tekniikkakeskus

HUOMIO! Tietokoneesi on lukittu turvallisuuden vuoksi allamainittujen syiden takia. Sinua syytetään kielletyn laittoman aineiston katselusta/säilytyksestä ja/tai levityksestä. Sinä olet rikkonut Suomen lakia ja sinua syytetään Suomen tasavallan rikoslain lakipykälän 161 edellyttämään rikokseen.

Suomen tasavallan rikoslain lakipykälä 161 edellyttää rangaistuksena vapausrangaistusta 2-8 vuotta.

Suomen tasavallan rikoslain korjauksien (i o. heinäkuuta 2013) ja Ihmisoikeuksien julistuksen mukaan rikkomistasi voidaan pitää tahattomina jos nämä rikkomiset on tehty ensimmäisen kerran ja sinua ei saateta rikosvastuuseen. Tämä ehto on mandollista toteuttaa jos sinä maksat sakon valtion kassaan. Sakot on maksattava 48 tunnin aikana rikoksen jäkeen. 48 tunnin kuluttua sinua vastaan nostetaan rikosasia.

Sakon määrä on €100. Sinä voit maksaa ainoastaan PaySafeCard-kortilla.

Liisa ei pääse käyttämään tietokonettaan, koska viesti peittää koko ruudun eikä siitä pääse ohi. Hän tietää, ettei ole tehnyt tietokoneellaan mitään laitonta, mutta ei keksi muutakaan keinoa kuin maksaa sata euroa viestissä osoitetulla tavalla. Ikävä kyllä, tekaistujen sakkojen maksaminen ei poista viestiä. Tällä niin sanotulla kiristyshaittaohjelmalla huijataan ihmisiltä rahaa. Sen saa pois koneelta kotikonstein, mikä tosin vaatii jonkin verran ammattitaitoa. Haittaohjelmat pääsevät tietokoneelle heikon tietoturvan takia. Ne käyttävät tietoturvaohjelmiston puutetta sekä ohjelmia, joita ei ole päivitetty pitkään aikaan. Ne leviävät myös sähköpostitse saastuneiden liitetiedostojen mukana. Siksi tuntemattomilta lähettäjiltä tulleiden viestien liitteitä ei koskaan kannata avata.

Miten suojaan älypuhelimeni?

- Mikäli saat tuntemattomasta numerosta tekstiviestin, jossa on nettiosoite, ei kannata vierailla kyseisellä sivulla.
- Asenna uusia sovelluksia eli appseja vain puhelimen omasta sovelluskaupasta.
- Pidä Bluetooth-yhteys päällä ainoastaan tarvittaessa.
- Näillä yksinkertaisilla keinoilla käytät puhelintasi turvallisesti.

Älypuhelinten tietoturva

Älypuhelimet ovat käytännössä pienikokoisia tietokoneita, joilla voi soittaa puheluita. Niihin voidaan asentaa sovelluksia eli ”appseja”, joilla voidaan selata internetiä, lukea ja kirjoittaa sähköpostia ja käsitellä tiedostoja. Älypuhelimia voidaan ajatella pienikokoisina tietokoneina myös tietoturvan kannalta. Ne saattavat sisältää luottamuksellisia tietoja ja niillä käytetään verkkopalveluja kuten pankkipalveluja ja sosiaalista mediaa. Tämän takia älypuhelimen tietojen turvaamiseen kannattaa kiinnittää huomiota samalla tavalla kuin kotitietokoneen tietoturvaan.

Älypuhelimen katoamiseen, varastamiseen, haittaohjelmatartuntaan tai rikkoontumiseen kannattaa varautua ottamalla puhelimen sisällöstä säännöllisesti varmuuskopio. Sen voi määritellä puhelimen asetuksista automaattiseksi, jolloin tärkeät tiedot ja kuvat eivät pääse katoamaan.

Älypuhelimille kehitetyt haittaohjelmat leviävät mm. Bluetooth-yhteyksien, multimediaviestien ja saastuneiden ohjelmien välityksellä. Ne voivat käyttäjän tietämättä kasvattaa puhelinlaskua, hävittää tai varastaa tietoa laitteesta ja vakoilla.

Salasana ja käyttäjätunnus

Moniin palveluihin kuten sähköpostiin tai Facebookiin vaaditaan käyttäjätunnus ja salasana, joilla niihin tunnistaudutaan. Palvelusta riippuen käyttäjätunnus voi olla keksitty nimimerkki tai oma sähköpostiosoite. Moniin sosiaalisen median palveluihin kirjaudutaan sähköpostiosoitteella, mutta profiiliin voidaan määritellä näkyviin käyttäjänimenä jokin muu, esim. etunimi tai lempinimi.

Nykyisin yhä useampiin palveluihin voidaan kirjautua jonkin toisen sosiaalisen median palvelun kuten Facebookin, Twitterin tai Googlen tunnuksella. Tällöin palvelu käy lukemassa profiilitiedot siitä palvelusta, jonka tunnuksella kirjauduttiin.

Salasana on ainoastaan käyttäjän itsensä tiedossa oleva kirjain- ja numeroyhdistelmä. Nimestään huolimatta salasana ei välttämättä ole sana. Joskus se voi koostua pelkistä numeroista kuten kännykän PIN-koodi. Yleensä nettipalveluiden salasanoissa tulee olla sekä isoja ja pieniä kirjaimia että numeroita, joskus myös erikoismerkkejä.

Lisäksi salasanan pitäisi olla niin helposti muistettava, ettei sitä tarvitsisi kirjoittaa paperille tai kuljettaa paperilla mukana. Mikäli joudut kirjoittamaan salasanan muistiin, älä kirjoita käyttäjätunnustasi samalle paperille. Jos paperi, johon olisit kirjoittanut tunnuksesi ja salasanasi, päätyisi vääriin käsiin, kuka tahansa pääsisi tietoihisi ja vaikka muuttamaan salasanasi, jolloin et enää itse pääsisi kirjautumaan palveluun.

Monissa nettipalveluissa käyttäjätunnuksena käytetään omaa sähköpostiosoitetta. Suojaa siis erityisen hyvin sähköpostisi salasana. Älä kirjoita sitä sähköpostiosoitteesi kanssa mihinkään muuhun nettipalveluun. Jos joku anastaa tunnuksesi johonkin nettipalveluun, esim. Facebookiin, voit aina palauttaa sen kertomalla palvelulle, että salasanasi on kadoksissa. Tällöin palvelu lähettää sähköpostiisi kertakäyttöisen salasanan tai linkin uuden salasanan luomiseen.

Hyvän salasanan tunnusmerkkejä:

- Se on tarpeeksi pitkä, mieluiten vähintään 8 merkkiä.
- Se sisältää isoja ja pieniä kirjaimia sekä numeroita.
- Se ei ole suoraan sanakirjasta löytyvä sana.
- Se ei ole käyttäjän osoite, syntymä- tai hääpäivä, auton rekisterinumero, perheenjäsenen tai lemmikin nimi tai muu helposti arvattava merkkijono.

Verkkopankkitunnukset

Tarvitset verkkopankkitunnukset maksaaksesi laskuja tietokoneella, tablettitietokoneella tai älypuhelimella. Tunnukset ovat henkilökohtaiset, joten voit tunnistautua niillä myös monissa muissa asiointipalveluissa. Pääset verkkopankkitunnuksillasi mm. tarkastelemaan sähköisiä reseptejäsi, hakemaan Kelan etuuksia, palauttamaan veroilmoituksesi ja ilmoittamaan muutoksista postiin tai maistraattiin. Näissä palveluissa verkkopankkitunnukset toimivat allekirjoituksenasi.

Verkkopankkitunnuksiin kuuluu yleensä pysyvä käyttäjätunnus sekä vaihtuvia tunnuslukuja. Mikäli kuljetat verkkopankkitunnuksia mukanasi, niitä ei kannata säilyttää samassa paikassa. Molempien tunnusten joutuessa vääriin käsiin pankkitilin tyhjentäminen on helppoa.

Noin

45%

ikäihmisistä ei pelkää internet-palvelun käyttäjäksi rekisteröitymistä.

Noin

50%

ikäihmisistä pitää tietokoneita luotettavina.

Liiat vaaratekijät, kuten virukset ja tietojen joutuminen vääriin käsiin, on 30% ikäihmisillä syynä, etteivät he käytä tietotekniikkaa.

Nordlund, Stenberg & Lempola : Tietoteknologian käyttö ja käyttämättömyyden syyt 75-89-vuotiailla. KÄKÄTE-projekti & LähiVerkko-projekti. 2014.

Mistä saan apua?

Mikäli epäilet, että pankkitunnuksesi ovat joutuneet vääriin käsiin, lukitse tunnukset heti. Soita pankkiin tai lukitse tunnukset verkkopankissa, jos vielä pääset sinne.

Jos epäilet, että tietokoneessasi on haittaohjelmia, suorita virustarkistus tietoturvaohjelmalla. Jos et itse onnistu, pyydä apuun vaikka sukulaista tai naapuria. Tehtävä saattaa osaavalle ihmiselle olla yksinkertainen, vaikka se sinusta tuntuisi monimutkaiselta. Jos turvaudut kaupallisen toimijan palveluksiin, löydät apua lähes joka kaupungista. Osa kaupallisista toimijoista voi huoltaa tietokoneesi etäyhteydellä, jolloin sinun ei tarvitse kantaa tietokonettasi minnekään.

Sanasto osa 3.

Bluetooth	Lyhyen matkan langaton viestintätekniikka. Monet tietokoneiden langattomat hiiret toimivat Bluetooth-yhteydellä.
Flash player	Ohjelma, jota käytetään usein animaatioiden ja elokuvien katseluun. Flash player kannattaa päivittää haavoittuvuuksien takia, mikäli tietokoneesi ehdottaa sitä.
Haavoittuvuus	Tietoturva-aukko, jonka avulla voi tehdä haittaa tietokoneelle. Haavoittuvuudet paikataan asentamalla haavoittuvuuksia sisältäviin ohjelmiin päivityksiä.
Haittaohjelma	Ohjelma, joka aiheuttaa ei-toivottuja tapahtumia tietokoneissa. Haittaohelmia on erilaisia, mm. mainosohjelmat, vakoiluohjelmat ja kiristysohjelmat. Haittaohjelmien poistamiseen on olemassa eri ohjelmia.
Hakkeri	Innokas tietokoneharrastaja. Nykykielessä usein myös henkilö, joka murtautuu laittomasti tietoverkkoon tai muihin tietokoneisiin.
Käyttöjärjestelmä	Tietokoneen keskeinen ohjelmisto, jonka päällä kaikki muut ohjelmat toimivat. Älylaitteiden yleisimmät käyttöjärjestelmät ovat iOS (Apple), Windows Phone (Lumia) ja Android.
Nigerialaiskirje	Sähköpostiviesti, jossa uhria pyydetään lähettämään rahaa vaikka tulevaa perintöä vastaan. Viesti on usein kirjoitettu taitavasti ja tunteisiin vetoavasti, mutta luvattuja rahoja ei ole olemassakaan.
Päivitys	Päivityksellä voidaan tarkoittaa kahta asiaa. Tässä vihkosessa päivityksellä tarkoitetaan ensimmäistä kohtaa. 1) Tietoteknisen laitteen käyttöjärjestelmän tai muun ohjelmiston päivittämistä uuteen versioon, joka korjaa ohjelmistossa olleita virheitä tai parantaa sen toimintaa. Käyttäjä voi itse päivittää laitteensa ohjelmistot tai antaa laitteen päivittää ohjelmistonsa automaattisesti. 2) Päivityksistä puhutaan myös sosiaalisessa mediassa. Esimerkiksi Facebook-päivitys tarkoittaa yksittäisen käyttäjän Facebook-palveluun kirjoittamaa viestiä tekemisestään tai jakamaa kuvaa ympäristöstään.
Sovellus, appsi	Tietokoneohjelma, joka toteuttaa tietyn tehtävän. Älylaitteissa esimerkiksi kalenteri, pelit ja herätyskello ovat “appseja”.
Tili	Käyttäjätunnuksen ja salasanan takana oleva palvelu, johon ulkopuoliset eivät pääse käsiksi, esim. sähköpostitili. Useimmiten nettipalveluiden tilit ovat maksuttomia, ellei toisin mainita.
Wi-Fi	Langaton internet-verkko, johon tietokoneet ja muut laitteet voidaan yhdistää ilman kaapeleita. Puhekielessä Wi-Fi ja WLAN tarkoittavat samaa asiaa.

Käytän melko paljon nettikauppoja. Selailen tarjontaa, vertaan hintoja ja tuotteita, jos olen jotain hankkimassa. Suunnittelen netin kautta elämääni, minne mennä ja mitä tehdä. Matkat, hotellit ja teatteriliput hankin netistä. Matkoilla katson suositut ravintolat, niiden menut ym. Raha-asiat hoidan tietenkin kaikki netissä. En ole käynyt pankissa vuosiin. Turva-asioissa olen myös tarkkana. En osallistu kilpailuihin tai mihinkään, jossa kysytään henkilötietoja tai meilejä. Ei pidä klikkailla kaikkea auki, jos ei tajua missä mennään. Ei pidä uskoa kaikkea, mitä luvataan tai kirjoitetaan. Virustorjunta hoituu perusohjelmalla, joka on netistä ilmaiseksi ladattu. On tähän asti riittänyt. Nettielämää on itselläni takana jo parikymmentä vuotta

Ritva, 67 vuotta

Olin ulkomailla. Olin sammuttanut kännykän ja avatessa en muistanut salasanaa, vaan kirjoitin sen aina väärin, kunnes känny lukkiutui. Eihän siinä auttanut muu kuin laittaa hotellin koneella sähköpostia tyttärelleni, joka sai puhelinyhtiöltä jonkun avauskoodin - huh!

Eeva, 73 vuotta

Pohdittavaksi:

Laske, kuinka monessa eri paikassa sinulla on salasana. Mikäli kirjaudut samoilla, esim. Google-tunnuksilla useaan paikkaan, ei jokaista tarvitse laskea erikseen. Myös matkapuhelimen PIN-koodi ja pankkikortin tunnusluku ovat salasanoja. Mieti, miten sinun olisi hyvä pitää tallessa kaikki salasanasi.

Koska käytännössä jokainen tietokoneen käyttäjä pohtii näitä asioita, tähän tarkoitukseen on kehitetty salasanojen hallintaohjelmistoja. Nämä ohjelmistot muistavat puolestasi ja mahdollistavat siten vaikeatkin salasanat. Erilaisia salasanojen hallintaohjelmistoja ovat esimerkiksi LastPass, KeePass ja suomalainen KEY. Niitä voi käyttää harkiten.

Tehtävän toteuttaminen ryhmässä: Keskustelkaa kokemuksistanne salasanojen käytöstä ja muistamisesta. Millaisia muistisääntöjä olette itselle rakentaneet? Milloin salasana on vaikein muistaa? Mikä helpottaisi asiaa? Hyvät ideat kannattaa laittaa jakoon, mutta muista olla paljastamatta omia salasanojasi.

Seuraavassa Netikkään numerossa aiheena on Tekijänoikeudet. Muista käydä netissä osoitteessa *www.netikäs.fi*. Sivuilta löytyy lisätietoa ja materiaaleja.

ISBN 978-952-5950-30-4 (paperinen) | ISBN 978-952-5950-31-1 (pdf)