Opinnäytetyö (AMK)

Tietojenkäsittelyn koulutusohjelma

Tietoliikenne

2014

Rami Pietikäinen

KOTITALOUDEN TIETOTURVA

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietoliikenne

Elokuu 2014 | 44 sivua

Esko Vainikka

Rami Pietikäinen

KOTITALOUDEN TIETOTURVA

Tämän opinnäytetyön tavoitteena on antaa perustietoa kansalaisille siitä, miten huolehtia käyttäjän omien laitteiden tietoturvasta. Monessa asiassa, muun muassa älypuhelimien käytössä, kuuluu nykyään ottaa huomioon tietoturvakysymykset. Opinnäytetyö toteutettiin käyttäen erilaisia internet-lähteitä, sekä omaa kokemusta tietoturva-alalta.

Työn empiirinen osuus koostuu suojauksen tärkeyden kattavasta paketista sekä eri tavoista suojata yksityisyyttään. Työn neljä liitettä antavat yleisiä vinkkejä laitteiden turvallisuuteen liittyen, ohjeita tietokoneen salaamisesta, tiedostojen palautusten helppoudesta sekä tiedostojen turvallisesta poistosta.

Opinnäytetyössä kerrotaan erilaisista viruksista ja haittaohjelmista sekä miten niitä vastaan voidaan suojautua torjuntaohjelmilla. Lisäksi työssä käsitellään miten voi ehkäistä tuhoja varmuuskopioilla, suojautua päivityksillä ja vahvoilla salasanoilla. Työssä annetaan tietoa palomuurin tehtävistä ja käyttöoikeuksien tärkeydestä.

Opinnäytetyöstä syntyi opas sekä perus- että kokeneemmillekin käyttäjille, jota kiinnostaa laitteiden tietoturva ja yksityisyys.

ASIASANAT:

Tietoturva, tietosuoja, salaus, asiakirjaturvallisuus, haittaohjelmat, yksityisyys

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business information Technology | Data communications

August 2014 | 44 pages

Esko Vainikka

Rami Pietikäinen

HOUSEHOLD INFORMATION SECURITY

The aim of this thesis is to provide basic information to the public on how to take care of their information security. There are currently many aspects to take into account on security issues. This thesis was carried out using a variety of internet sources and experience in the information security sector.

The empirical part consisted of a comprehensive package about the importance of the data security and the different ways to protect user privacy. As a side product, the thesis contains tips for encryption, tips for easy file restore, and safe file removal.

In this thesis I bring out different kinds of viruses and malware and how to protect against them with prevention programs. Also the thesis deals with ways to prevent damages with backups and how to protect with software updates and strong passwords. The thesis provides information on the firewall functions and the importance of access rights.

The thesis has a guide for basic users and for more experienced users who are interested in the security and privacy of devices.

KEYWORDS:

Data security, privacy, encryption, document security, malware, privacy

SISÄLTÖ

LIITTEET

KUVAT

TAULUKOT

1 JOHDANTO

Yllättävän yleinen käsitys on, että jos koneella ei ole mitään salattavaa, ei tarvita hyvää suojaa tietokoneeseen. Tuolloin on hyvä kysyä itseltään: ”Mitä jos tietoni häviävät tai mitä jos joku näkee jokaisen näppäimenpainellukseni?”

Ihmisten tietoisuus internetin vaaroista on yleistynyt. Monet tunnistavat sähköpostin roskapostit roskaposteiksi, mutta rikolliset keksivät koko ajan uusia tapoja huijata käyttäjiä eri tavoin ja ammattimaisemmin. Tämä tekee joskus tunnistamisesta erittäin vaikeaa. Pelkästään roskapostin tunnistaminen ei riitä, sillä internet ja huijausten eri tavat ovat tuoneet monia muitakin vaaroja, joista tulee olla perillä.

Opinnäytetyön tärkeimpänä tavoitteena on tutustuttaa lukija eri tapoihin suojata omat yksityiset tietonsa. Työn tutkimusote on kvalitatiivinen ja tutkimus on konstruktiivinen, ja sen tuloksena on annettu ohjeita tietojen suojaamiseen.

2 TIETOTURVA KÄSITTEENÄ

Tietoturvalla tarkoitetaan tietojen suojaamista muun muassa rikoksia ja laitevikoja vastaan. Hyvässä tietoturvassa käyttäjän omat tiedot, järjestelmien suojaukset, palvelut sekä tietoliikenneyhteydet ovat suojattuina. Näiden suojaamisessa tavoitteena on estää murtoja, huijauksia ja väärinkäyttöjä.

Tietoturva on todella laaja aihe. Kaikelle tietoturvaan liittyvällä pyritään kolmeen tavoitteeseen, joka kuvataan CIA-kolmioksi (Taulukko 1). CIA-mallissa on kolme osatekijää – luottamuksellisuus, eheys ja saatavuus.

Taulukko 1. Ohjeita viestinnän suojaamiseen (Viestintävirasto 2013).

Toimenpide	Luottamuksellisuus	Eheys	Saatavuus
Sähköpostin salaus	Parantaa	Ei vaikutusta	Heikentää
Sähköinen allekirjoitus	Ei vaikutusta	Parantaa	Ei vaikutusta
Hyvän salasanan käyttö/ PIN-koodit	Parantaa	Ei vaikutusta	Heikentää
Ohjelmistojen ajantasaiset päivitykset	Parantaa	Parantaa	Parantaa
WLAN-verkon avoimuus	Heikentää	Heikentää	Parantaa
Tiedon tai koko kovalevyn/muistitikun salaaminen	Parantaa	Ei vaikutusta	Heikentää
Yleisimpien pilvipalveluiden käyttö	Heikentää	Ei vaikutusta	Parantaa
WLAN-verkon WPA 2 salaus	Parantaa	Ei vaikutusta	Ei vaikutusta

CIA-kolmion luottamuksellisuudella (Confidentiality) tarkoitetaan sitä, että omia yksityiseksi tarkoitettuja tietoja ulkopuoliset eivät saa nähdä. Näitä voivat olla esimerkiksi omat palkkatiedot tai yrityksen liikesalaisuudet. Omien henkilökohtaisten tietojen jakamisen suhteen tulee olla varovainen. Koskaan ei kannata luovuttaa omia tietoja epämääräisille sivuille. Vääriin käsiin joutuneen sosiaaliturvatunnnuksen tai luottokortti- ja pankkitietojen riskinä voi olla identiteettivarkaus tai luottokorttien väärinkäyttö.

Eheydellä (Integrity) tarkoitetaan sitä, että vain tietyillä henkilöillä on oikeus käyttää tietoa ja muokata sitä, eikä tieto muutu matkalla. Hyvänä esimerkkinä

eheyden menetyksestä ovat kotisivut, jotka ovat muuttuneet jonkun toisen tahon, esimerkiksi hakkerin, toimesta erilaisiksi.

Saatavuus (Availability) CIA-kolmiossa tarkoittaa tiedon saatavuutta aina, kun sitä tarvitaan. Kiintolevyjen rikkoutuminen ja nettiyhteyksien katkeileminen heikentävät saatavuutta. Pilvipalvelujen avulla omiin tietoihin pääsee paikasta riippumatta aina käsiksi, kunhan käytössä on internet-yhteys, ja palveluntarjoaja on huolehtinut saatavuudesta omalta osaltaan.

Käytön mukavuus ja tietoturvallisuus eivät kulje käsi kädessä. Langattomien verkkojen avulla tietokoneen ei tarvitse olla johdon päässä ja kaapelien käyttö vähentyy. Tietoturvan osalta langaton verkko ei koskaan pääse langallisen verkon tasolle.

3 VIRUKSET JA HAITTAOHJELMAT

Haittaohjelmien tarkoitus on hankkia henkilökohtaista tietoa, päästä käsiksi yksityisiin järjestelmiin tai häiritä tietokoneen toimintaa. Vuonna 2012 järjestelmien haittaohjelmista 60-70 prosenttia tuli käyttäjien napautuksilla (Microsoft Malware Protection Center 2012).

Virukset harvoin tuhoavat tai sekoittavat tietokoneita. Sen sijaan niiden tehtävä on usein rahan keruu tai henkilötietojen kalastus. Haittaohjelmiin ja viruksiin tulee aina suhtautua vakavasti, vaikka tietokoneelle päässyt virus olisi harmiton.

Virusten- ja haittaohjelmien tekijät kohdentavat ohjelmiaan niihin järjestelmiin, joissa on paljon käyttäjiä. Tietokoneissa tämä tarkoittaa Windows-käyttöjärjestelmiä. Googlen Android on tällä hetkellä suosituin älypuhelinten käyttöjärjestelmä, joten se on myös suosituin kohde puhelimissa. Windows-käyttöjärjestelmistä Windows XP on vielä erittäin suosittu kohde. Jopa 26% internetiin yhdistetyistä tietokoneista sisältää Windows XP:n (Zdnet 2014).

Antivirus- eli virustorjuntaohjelmista kuvitellaan, että kun sen on asentanut, ei tarvitse enää murehtia viruksista ja että ne pitävät koneen puhtaana. Nämä ohjelmat vaativat kuitenkin huomiota: tilauksen jatkuminen, päivitykset ja satunnaiset tarkistukset pitävät huolta siitä, että laitteet pysyvät puhtaana.

3.1 Haittaohjelmien perheet

Haittaohjelmien tyyppejä on monia. Jokainen erottuu toisistaan siten, miten ne toimivat.

Virus

Virukset ovat haittaohjelmista tunnetuimpia. Ne pyrkivät aina levittäytymään moneen paikkaan tehden itsestään kopioita, jolloin virus pyrkii aiheuttamaan vahinkoa tietokoneeseen poistamalla tiedostoja (Tietokonevirus 2013).

Mato

Madot eroavat viruksista hieman. Kun mato on päässyt järjestelmään, se alkaa kopioida itseään kunnes kiintolevy on täynnä. Silloin mato ottaa koneen hallintaansa ja varastaa käyttäjän tietoja. Tämän jälkeen mato levittäytyy muihin verkon laitteisiin ruuhkauttaen niitä. Niihin kuuluu esimerkiksi ulkoinen kiintolevy, johon laitetaan varmuuskopioita. Tämän takia on tärkeää, ettei pidä varmistukseen tarkoitettua kiintolevyä koko ajan kiinni tietokoneessa (BBC 2010).

Troijalainen

Troijalaiset usein naamioivat itsensä hyödyllisiksi ohjelmiksi, joita käyttäjä asentaa koneelleen. Asennuksen jälkeen ne aktivoituvat kohdejärjestelmässä luoden takaportteja hakkereille sekä varastavat, poistavat ja muokkaavat tietoja (Kaspersky 2014).

Tämän takia on tärkeätä tarkistaa muualtakin kuin vain valmistajan sivuilta, mitä ohjelma oikeasti tekee. Internetistä ja keskustelupalstoilta saa hyviä tietoja, tekeekö ohjelma sitä, mitä se väittää tekevänsä.

Spyware

Spywaren eli vakoiluohjelman päästyä järjestelmään se alkaa kerätä tietoa itse järjestelmästä, käyttäjän tunnuksista ja selainten käytöstä. Vakoiluohjelmat pääsevät järjestelmiin pääosin käyttäjän lataamilla ohjelmilla (BBC 2012).

Adware

Mainosohjelmia kutsutaan Adwareksi. Ne ovat vähiten vaarallisia haittaohjelmista. Niitä ei kuitenkaan tule vähätellä. Ne esittävät pääosin käyttäjälle mainoksia, mutta ne voivat mainosten avulla huijata käyttäjää asentamaan muita haitallisia ohjelmia, kuten spywareja (Adware 2014).

Rootkit

Rootkitit ovat vaarallisimpia haittaohjelmia. Niiden aikomuksena on pyrkiä saamaan tietokoneen järjestelmävalvojan oikeudet ja piilottaa itsensä. Rootkitit voivat antaa hyökkääjälle rajattomat oikeudet tietokoneeseen (Zsecurity 2009).

Ransomware

Kiristysohjelmat (Ransomware) nimensä mukaisesti kiristävät uhreja eri tavoin saadakseen rahaa. Useasti kiristysohjelmat säikyttelevät uhreja maksamaan vääristä virustorjunnoista.

Kiristysohjelmat voivat estää käyttäjän pääsyn laitteeseen ja voivat jopa salata käyttäjän tiedot kunnes käyttäjä on maksanut lunnaat. Lunnaiden maksaminen ei välttämättä avaa salattua järjestelmää, vaan uhrin toivotaan maksavan useammin vaaditun summan. Tunnetuin kiristysohjelma on Suomessakin tunnettu poliisivirus (Koivula & Tuomola 2014, 10).

3.2 Suojaus haitallisia ohjelmia vastaan

Virustorjunta pitää huolen siitä, että koneella ei ole aktiivisia haittaohjelmia. Tunnetuimpia maksullisia virustorjuntaohjelmia ovat muun muassa F-secure, Eset ja Norton. Ilmaisista torjuntaohjelmista tunnetuimmat ovat avast!, AVG, sekä Microsoftin oma Security Essentials. Ilmaiset torjuntaohjelmat tuovat koneelle ainoastaan perusturvaa, mutta soveltuvat yksityiseen käyttöön.

Tietokoneella voi olla ainoastaan yksi virustorjuntaohjelma, jossa on reaaliaikainen suoja. Mikäli koneelle asentaa useamman ohjelman se hidastaa käyttöä huomattavasti. Tämä johtuu siitä, että molemmat torjuntaohjelmat haluavat tarkastaa samoja tiedostoja tartunnoilta.

Pelkkä virustorjunta tarkistaa usein ainoastaan virukset, eli muut haitalliset ohjelmat säilyvät koneilla käyttäjän tietämättä. Tämän takia on hyvä olla myös muita haittaohjelmia poistavia ohjelmia. Malwarebytes on yksi tunnetuimmista ohjelmista niiden poistoon. Malwarebytes tunnistaa, poistaa, sekä estää haittaohjelmien leviämisen. HijackThis-niminen ohjelma on yksi tehokkaimista poisto-

ohjelmista, mutta se voi tehdä paljon tuhoa kokemattomilla käyttäjillä. Kolmas hyvä ohjelma on Combofix, joka on käytettävyydeltään helpoin.

Kaikki kolme ohjelmaa ovat tehokkaita haittaohjelmien poistajia ja ovat myös ilmaisia. Malwarebytesistä on myös maksullinen versio, jolloin mukaan saa reaaliaikaisen suojauksen.

Parhaan suojan saa käyttämällä mediaa, johon ei pysty kirjoittamaan tietoa. CD- tai DVD-levyiltä käynnistyvät käyttöjärjestelmät antavat näin ollen parhaan mahdollisen suojan haittaohjelmia vastaan. Tämä taas tuo käytettävyyteen ongelmia, koska ne eivät ”muista” käyttäjien tekemiä asetuksia.

4 PALOMUURI

Tietokoneissa on tuhansia portteja, joiden avulla pystyy käyttämään tiettyjä verkon ohjelmia, kuten esimerkiksi internet-selainta. Rikolliset etsivät avoimia portteja, joiden avulla he saavat pääsyn uhrin koneeseen. Palomuurien tehtävänä on estää ja suojata verkkoa luvattomilta hyökkäyksiltä ja pitää ylimääräiset portit suljettuina. Palomuuria voi siis kuvailla muurina, joka päästää tai pysäyttää liikenteen. Jokaisesta estosta jää merkintä palomuurin lokiin. Palomuuri ei suojaa sähköpostin kautta tulevia viruksia, vaan ainoastaan hyökkäyksiä ja ohjelmia. Hyvässä tietoturvassa koneissa on molemmat, sekä laitepalomuuri että ohjelmallinen palomuuri.

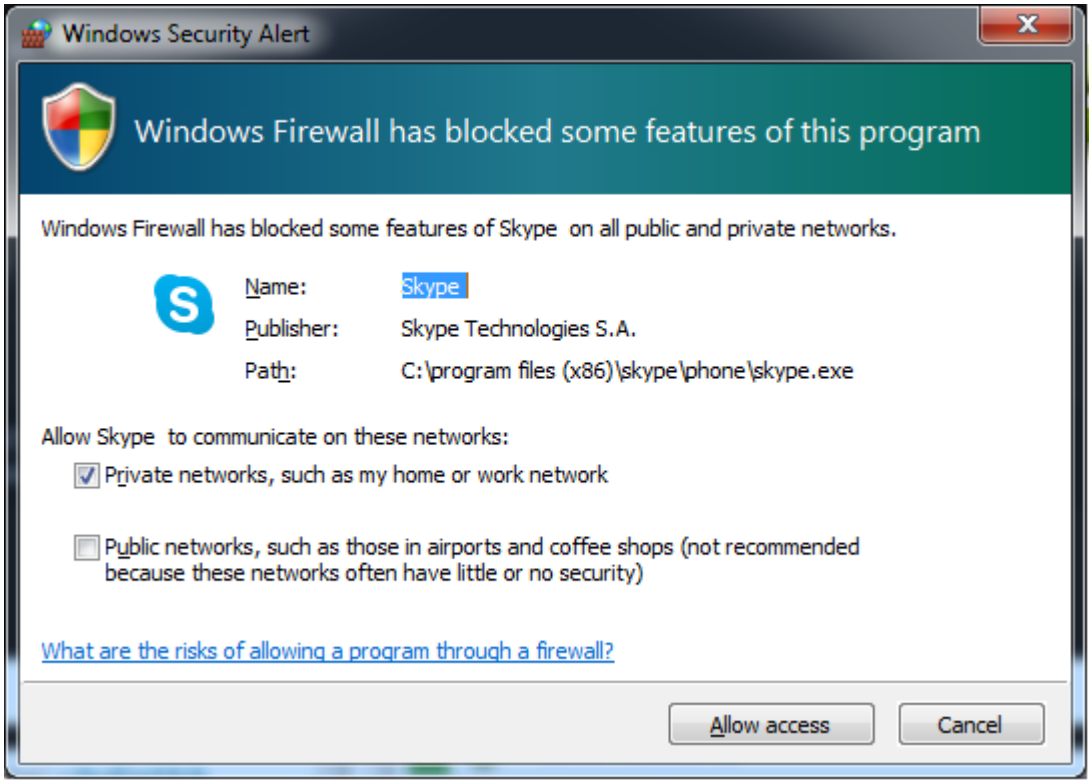
4.1 Laitepalomuuri

Laitepalomuuri on erillinen laite, jonka tarkoituksena on rajoittaa sisäänpäin tulevaa liikennettä. Tämä ominaisuus on monessa ADSL-reitittimissä, joten uutta laitetta ei välttämättä tarvitse hankkia. Usein laitepalomuuri on varmempi kuin ohjelmallinen, koska sitä ei voida sammuttaa haittaohjelmien kautta. Lisäksi laitepalomuuri suojaa kaikkia lähiverkon koneita.

4.2 Ohjelmallinen palomuuri

Ohjelmallisten palomuurien tärkein tehtävä on varoittaa käyttäjiä sovellusten yhteydenottoyrityksistä. Kun ohjelmallinen palomuuri havaitsee uuden sovelluksen, palomuuri kysyy sallitaanko vai estetäänkö sovelluksen pääsy internetiin. Tämä suojaa virusten yhteydenottoyrityksiltä ulospäin. Rajoitetuilla käyttäjäoikeuksilla voidaan varmistaa, ettei haittaohjelma pysty sammuttamaan palomuu-

ria. Ohjelmalliset palomuurit osaavat estää myös tulevia hteyspyyntöjä.



Kuva 1. Windowsin palomuuri.

Ohjelmallinen palomuuri suojaa hyvin lähiverkkoa. Jos jokin kotiverkon tietokone on saastunut, virukset eivät leviä muihin verkon koneisiin. Tätä laitepalomuuri ei yleensä tee, ellei kaikkia lähiverkon koneita ole kytketty palomuurin eri verkkoliitäntöihin. On hyvä muistaa, että ohjelmallisia palomuureja saa tietokoneissa olla käytössä vain yksi. Suosituimmat ilmaiset palomuurit ovat Comodo sekä ZoneAlarm. Myös Windowsin mukana tulee oma palomuuri. Ohjelmalliset palomuurit kysyvät uuden ohjelman käynnistyessä lupaa päästä verkkoon (Kuva 1).

4.3 NAT

Network Address Translation (NAT) eli osoitteenmuunnos on tekniikka, jonka avulla piilotetaan sisäverkko ulkoverkosta. Tämän avulla moni tietokone voi

käyttää yhtä julkista IP-osoitetta ja näin ulkoapäin ei näe, montako tietokonetta esimerkiksi sisäverkossa on.

5 VARMUUSKOPIOT

Varmuuskopiot pitävät tiedot suojattuina, jos alkuperäisille tiedostoille tapahtuu jotakin. Myös virukset osaavat salakirjoittaa käyttäjän tiedostot tehden niistä käyttökelvottomia. Tästä syystä varmuuskopion mediaa, kuten ulkoista kiintolevyä, ei kannata pitää aina kiinni tietokoneessa, vaan irroittaa se heti, kun varmuuskopiot on otettu.

Varmuuskopioita tulisi ottaa tietokoneen lisäksi myös tableteista ja puhelimista. Niitä voi kopioida esimerkiksi toiselle tietokoneelle, USB-muistille tai pilveen. Hyvä varmuuskopio on silloin, kun tiedot ovat turvassa vaikka talo palaisi. Pilvipalveluissa tulee olla hyvät suojaukset ja palvelun olla luotettava.

Ilmaisia varmuuskopiointiohjelmia ovat esimerkiksi Windowsin oma varmuuskopiointiohjelma ja avoimen lähdekoodin Cobian. Varmuuskopioinnin voi tehdä myös itse helposti kopioimalla ja liittämällä tiedostot esimerkiksi ulkoiselle kiintolevylle tai polttamalla ne CD/DVD-levylle.

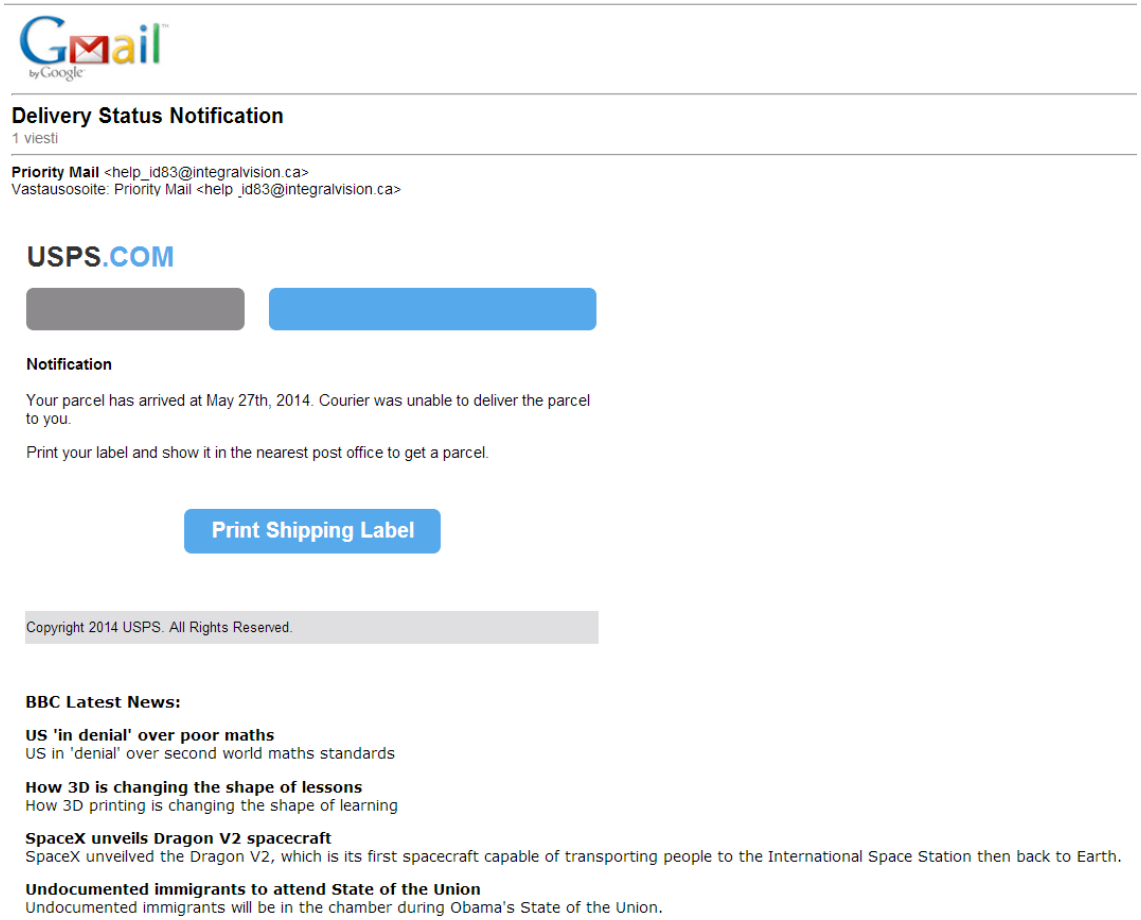
6 SÄHKÖPOSTI

Sähköposti on iso osa kansalaisen tietoturvaa. Postissa voi olla arkaluontoisia viestejä ja liitetiedostoja, sekä sen kautta pystyy palauttamaan unohtuneita salasanoja moniin paikkoihin, kuten esimerkiksi Facebookiin.

6.1 Roskapostit

Moneen paikkaan täytyy rekisteröityessä lisätä oma sähköpostiosoite. Jos haluaa pitää sähköpostin siistinä, mikään ei estä luomasta useampaa sähköpostitiliä. Oma henkilökohtainen sähköposti virallisille posteille ja toinen sähköposti kaikille muille viesteille on hyvä keino pitää saapuvat viestit järjestyksessä. Kuvassa 2 on esimerkki roskapostista.

Verkkosivut voivat myydä henkilökohtaisia tietojasi, esimerkiksi sähköpostin osoitteen eteenpäin. Jos sivusto näyttää epäilyttävältä, hyvänä keinona on luoda väliaikainen sähköposti. 10minutemail.com on sivusto, jossa sähköposti on ainoastaan 10 minuuttia voimassa. Tämän jälkeen postia ei enää pääse tarkastamaan.



Gmail by Google

Delivery Status Notification

1 viesti

Priority Mail <help_id83@integralvision.ca>
Vastausosoite: Priority Mail <help_id83@integralvision.ca>

USPS.COM

Notification

Your parcel has arrived at May 27th, 2014. Courier was unable to deliver the parcel to you.

Print your label and show it in the nearest post office to get a parcel.

Print Shipping Label

Copyright 2014 USPS. All Rights Reserved.

BBC Latest News:

US 'in denial' over poor maths
US in 'denial' over second world maths standards

How 3D is changing the shape of lessons
How 3D printing is changing the shape of learning

SpaceX unveils Dragon V2 spacecraft
SpaceX unveilved the Dragon V2, which is its first spacecraft capable of transporting people to the International Space Station then back to Earth.

Undocumented immigrants to attend State of the Union
Undocumented immigrants will be in the chamber during Obama's State of the Union.

Kuva 2. Roskapostia USPS:n nimellä.

6.2 PGP

PGP tulee sanoista Pretty Good Privacy. Se on ilmainen ja erittäin tehokas salausohjelma, jonka avulla voi salata sähköpostiliikennettä. Siitä on tehty versiot lähes kaikille käyttöjärjestelmille. PGP vaatii toimiakseen sähköpostiohjelman tietokoneelle, eli selaimen kautta tämä ei toimi automaattisesti.

PGP perustuu julkisiin ja yksityisiin avaimiin. Julkisia avaimia käytetään viestien salaukseen, yksityisiä salauksen purkamiseen. Käyttäjälle lähetetyt viestit täytyy salata käyttäjän antamalla avaimella.

7 IDENTITEETTIVARKAUKSET JA HUIJAUKSET

Varastetuilla henkilötiedoilla tehdään paljon petoksia. Sonera on kertonut että väärillä identiteeteillä tehdään paljon liittymien tilauksia. Riittää että huijarilla on uhrin henkilötiedot sekä osoite (Åström-Kupsanen, M 2012).

Käyttäjien tiedot kiinnostavat rikollisia. Vuonna 2011 tapahtui mahdollisesti historian suurin tietomurto. Sonyn Playstation network -palvelun käyttäjien tiedot päätyivät hakkereiden käsiin. Käyttäjiä oli tuolloin 77 miljoonaa. Hakkerit saivat käsiinsä käyttäjien nimet, osoitteet, salasanat ja osittain pankkikorttien tietoja. (PlayStation Network -katkos 2014.)

Internetin mainokset lupaavat monia asioita. Käyttäjiä pyritään hujaamaan muun muassa asentamaan ohjelmia, napauttamaan mainoksia ja antamaan pankkitietojaan sekä yhteystietojaan.

7.1 Huijaustapoja

Huijaustapoja on monia. Sähköpostin kautta tulevat huijaukset ovat erittäin yleisiä. Internetin kauppapaikoissa voi tapahtua huijauksia, joten tulee olla tarkkana, mistä tilaa. Tietojen kalastusta kohdistuu esimerkiksi verkkopankkitunnuksiin.

Valeturvaohjelmat huijaavat käyttäjiä uskomaan, että koneella on hyvä virustorjuntaohjelma. Ne lataavat erilaisia haittaohjelmia ja ilmoittavat löytäneensä niitä. Mikäli käyttäjä haluaa päästä haittaohjelmista eroon, pitäisi ohjelmasta maksaa. Huijausohjelmat huijaavat uhreja myös mainosten kautta kuten kuvassa 3 on esitetty.

Kuva 3. Mainos haitallisesta ohjelmasta.

7.2 Huijausten ennaltaehkäisy

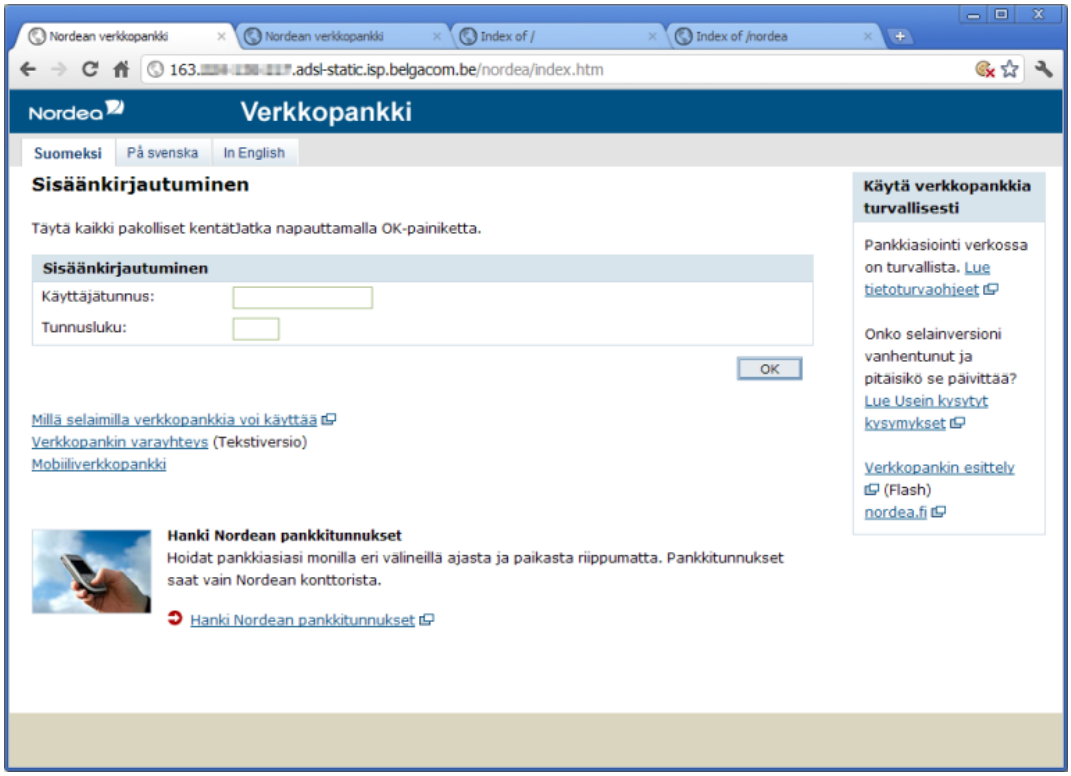
Kaikki tietokoneella olevat arkaluontoiset tiedot tulisi salata. Tämän opinnäytetyön liitteissä ohjeistetaan kuinka tämä tehdään. Koko kiintolevyn salaaminen ei tässä tapauksessa auta, sillä salaus aukaistaan tietokoneen käynnistyessä (Norton Identity Theft 2014).

Selainten lisäosat tulisi tarkistaa ja poistaa kaikki ylimääräiset. Mikäli mainokset haluaa kokonaan pois näkyvistä, ilmainen ”Adblock” -lisäosa hoitaa ne pois. Näin käyttäjät eivät vahingossakaan paina mainoksia. Se nopeuttaa myös internet asiointia, koska selaimen ei tarvitse ladata kaikkea sivun sisältöä. Tämä lisäosa tunnetaan Microsoftin Internet Explorer –selaimessa nimeltä EasyList.

Omia tietoja pyydetään usein kirjaamaan erilaisiin palveluihin. Omien luottamuksellisten tietojen, kuten henkilötunnusten ja syntymäajan antamisessa tulee olla tarkkana, etteivät ne päädy vääriin käsiin.

Verkkosivujen avaamiset kannattaa tehdä itse kirjoittamalla niiden osoitteet selaimeen. Sähköpostien kautta tulleet linkit voivat huijata käyttäjiä uskomaan, että ne ovat esimerkiksi linkkejä oman pankin sivuille, mutta ne voivat todellisuudessa ollakin linkkejä huijarin tekemälle, vastaavan näköiselle tietojen kalastelu-sivulle. Pankkiasioinnissa tulee olla erittäin tarkkana, että sivun osoiterivillä on oikea osoite (Kuva 4). Nordean huijaussivun huomaa osoiterivillä olevasta osoitteesta joka ei viittaa Nordean sivuihin.

Roskapostilta vaikuttavaa postia ei tule koskaan aukaista. Jos näin tekee, mahdolliset liitteet voivat sisältää viruksia tai ohjelmien tietoturva-aukkoja hyväksikäyttäviä haittaohjelmia jotka mahdollistavat niiden pääsyn laitteeseen.



Kuva 4. Nordea pankin huijaussivu (Dataprotectioncenter 2011).

8 KÄYTTÖOIKEUDET

Virusten leviäminen hankaloituu huomattavasti, mikäli tietokonetta käytetään tavallisen käyttäjän oikeuksilla. Järjestelmävalvojalla on oikeudet tehdä mitä vain. Tämän takia Windowsiin suositellaan tehtäväksi kaksi käyttäjätunnusta: järjestelmävalvojan oikeuksilla oleva käyttäjä sekä normaalikäyttäjän oikeuksilla oleva käyttäjä.

Aina kun Windowsia käytetään, tulisi kirjautua normaalikäyttäjän oikeuksilla. Vasta kun tietokoneeseen tehdään muutoksia, kysytään järjestelmävalvojan tunnuksia. Näin tietokoneelle ei asennu mitään ylimääräisiä ohjelmia vahingossakaan. Mikäli virus pääsee koneelle, se pääsee leviämään yhtä pitkälle, kuin mitä tartunnan saaneen käyttäjän oikeudet sallivat (Computer virus 2014).

9 SOVELLUKSET JA NIIDEN TIETOTURVA

Nykyajan laitteissa on monia sovelluksia. Haittaohjelmia voi olla melkein millä tahansa verkkosivulla, mikäli koneessa on paikkaamattomia turva-aukkoja. Usein ne tulevat mainosten kautta tai ne on istutettu tietoturvamurron yhteydessä.

9.1 Päivitykset

On hyvä ottaa selvää omista ohjelmista ja pitää ne päivitettyinä. Päivitykset ovat ohjelmistoihin tehtyjä lisäyksiä tai muutoksia, jotka korjaavat ongelmia ja parantavat tietokoneen toimintaa ja tietoturvaa. On tärkeää, ettei päivitä ainoastaan käyttöjärjestelmää, vaan ohjelmat on myös pidettävä ajan tasalla. Käyttöjärjestelmien ja ohjelmien tulisi aina olla päivitettynä uusimpaan vakaaseen versioon. Erityisesti selaimet ovat tärkeässä asemassa, sillä selainlaajennukset ovat yleisimpiä sovelluksia, joita vastaan hyökätään. Yleisimmät hyökkäykset kohdistuvat Java-, Quicktime- sekä Flash-laajennuksiin (Cisco 2014).

Virustorjuntaohjelmat päivittävät usein itse itseään, mutta aina silloin tällöin on hyvä varmistaa, että niissä on uusimmat päivitykset.

Windows-käyttöjärjestelmissä on käytössä Windows Update, jonka avulla käyttöjärjestelmä pysyy ajan tasalla. Updaten ajantasaisuus tulisi tarkistaa aika-ajoin. Tämän lisäksi on hyvä varmistaa, että käytössä on viimeisin Service Pack. Service Pack on kokoelma päivityksiä ja korjauksia.

9.2 Windows XP

Windows XP:n tuki loppui 8.4.2014. Tuen päättyminen tarkoittaa sitä, että Windowsille ei enää kehitetä uusia korjauksia haavoittuvuuksia vastaan. Tämä tekee XP:stä erittäin haavoittuvaisen eikä sitä suositella enää käytettäväksi. Tämä käyttöjärjestelmä on silti edelleen erittäin suuressa suosiossa ympäri maailmaa.

Heti 4 päivää tuen päättymisen jälkeen XP oli laajan hyökkäyksen kohteena. Vielä huhtikuun 2014 alussa jopa 25% maailman tietokoneista sisälsi pian vanhenevan käyttöjärjestelmän (The Telegraph 2014).

Yleisimmät hyökkäykset XP:tä kohtaan ovat tietoturva-aukot sekä tietoturvan huijausohjelmat. Vaikka tietokoneessa olisi hyvä virustorjunta, se ei riitä suojaamaan vanhentuneen käyttöjärjestelmän aukoilta tai käyttäjän asentamilta haittaohjelmilta.

10 SALASANAT

Salasanojen turvallisuus on erittäin tärkeää. Niiden avulla saa pääsyn tietoihin, joihin ainoastaan kyseisen käyttäjän on tarkoitus päästä. Liian usein käytetään yhtä salasanaa moneen paikkaan. Tämä luo vakavan tietoturvariskin. Mikäli tämä yksi salasana päätyy rikollisten haltuun, niitä saatetaan kokeilla muihin palveluihin.

Rekisteröidyttäessä uusiin palveluihin saatetaan kysyä turvakysymyksiä ”unohditko salasanasi”-osioon. Näihin ei välttämättä kannata laittaa oikeita tietoja, vaan niitä tietoja, jotka vain itse tietää. Jos mahdollista, kannattaa laatia ennemmin oma kysymys, sillä se rajoittaa ulkomaalaisia hakkereita ymmärtämästä kysymystä. Esimerkkinä oman lapsen nimen käyttäminen ”unohditko salasana”-osiossa on erittäin huono valinta, sillä internetin käytön yleistyessä rikolliset voivat löytää lapsen nimen helposti.

10.1 Yleisimmät salasanat

Yleisimmät salasanat ovat olleet joka vuosi helposti arvattavia. Suosituimpia suomalaisia salasanoja ovat olleet

- 123456
- perkele
- johanna
- qwerty
- nallepuh
- rasmus (Domnik 2011).

Listalla olevat salasanat on kerätty Suomen historian suurimmasta tietovuodosta (Lehto, E. & Kjellberg, H 2011).

10.2 Salasanan murtamistekniikat

Salasanan murtoihin on olemassa kaksi eri vaihtoehtoa. Ensimmäinen on sanakirjahyökkäys, joka kokeilee sanakirjaan syötettyjä sanoja kunnes oikea salasana on löytynyt. On erittäin tärkeää, ettei käytä mitään selkokielistä salasanaa missään. Toinen keino on Brute force. Brute force tarkoittaa ”raakaa voimaa”. Se kokeilee järjestyksessä kirjaimin (isot ja pienet), numeroin ja mahdollisesti erikoismerkein niin kauan kunnes se löytää oikean salasanan. Se on hidas keino selvittää salasana. Mitä pidempi suojausavain on, sitä kauemmin murtaminen kestää.

10.3 Vahva salasana

Salasanoina ei tulisi käyttää helposti arvattavia sanoja, esimerkiksi nimiä tai kadun nimiä. Vahva salasana

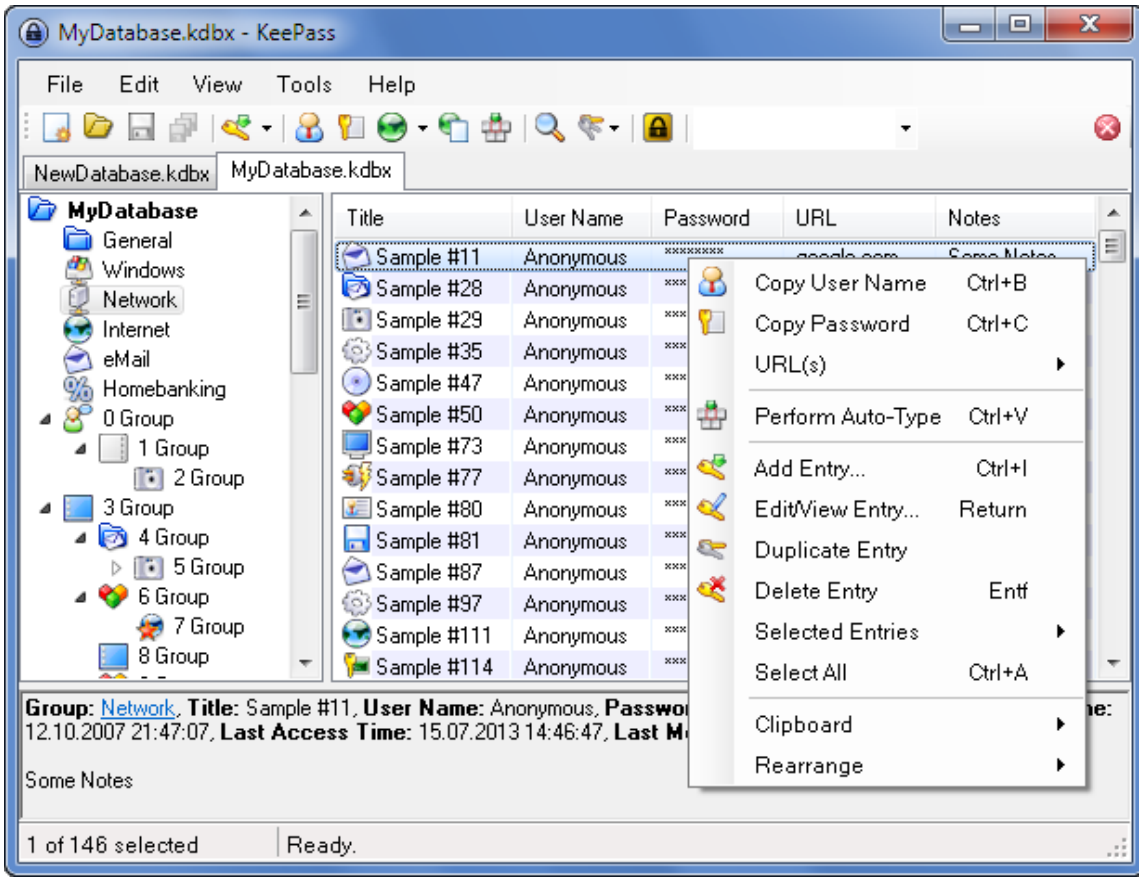
- on vähintään 15 merkkiä pitkä
- sisältää numeroita
- sisältää erikoismerkkejä, kuten !, ?, .
- sisältää isoja ja pieniä kirjaimia
- ei ole aiempien salasanojen kaltainen
- ei sisällä käyttäjänimeä
- ei ole ystävän tai perheenjäsenen nimi
- ei ole selväkielinen sana
- ei ole yleinen nimi
- ei ole muiden pääteltävissä
- vaihtuu aika-ajoin uuteen.

10.4 Salasanan palautus

Mikäli salasana unohtuu, voi sen usein palauttaa eri tavoin. Yleisin on sähköpostin kautta palautettava salasana. Matkapuhelinten kautta palautettava salasana yleistyy. Esimerkiksi Google käyttää tätä mahdollisuutta.

10.5 Tallennus

Salasanoja kertyy koko ajan enemmän ja enemmän ja näiden muistamisesta voi tulla ongelmia. Varsinkin, kun niitä tulisi vaihtaa aika-ajoin. Tähän voi käyttää apuna ohjelmia, joka tallettavat käyttäjän salasanat yhden salasanan alle. Näistä yksi on KeePass (Kuva 5). Keepass on avoimen lähdekoodin ohjelma salasanojen hallintaan.

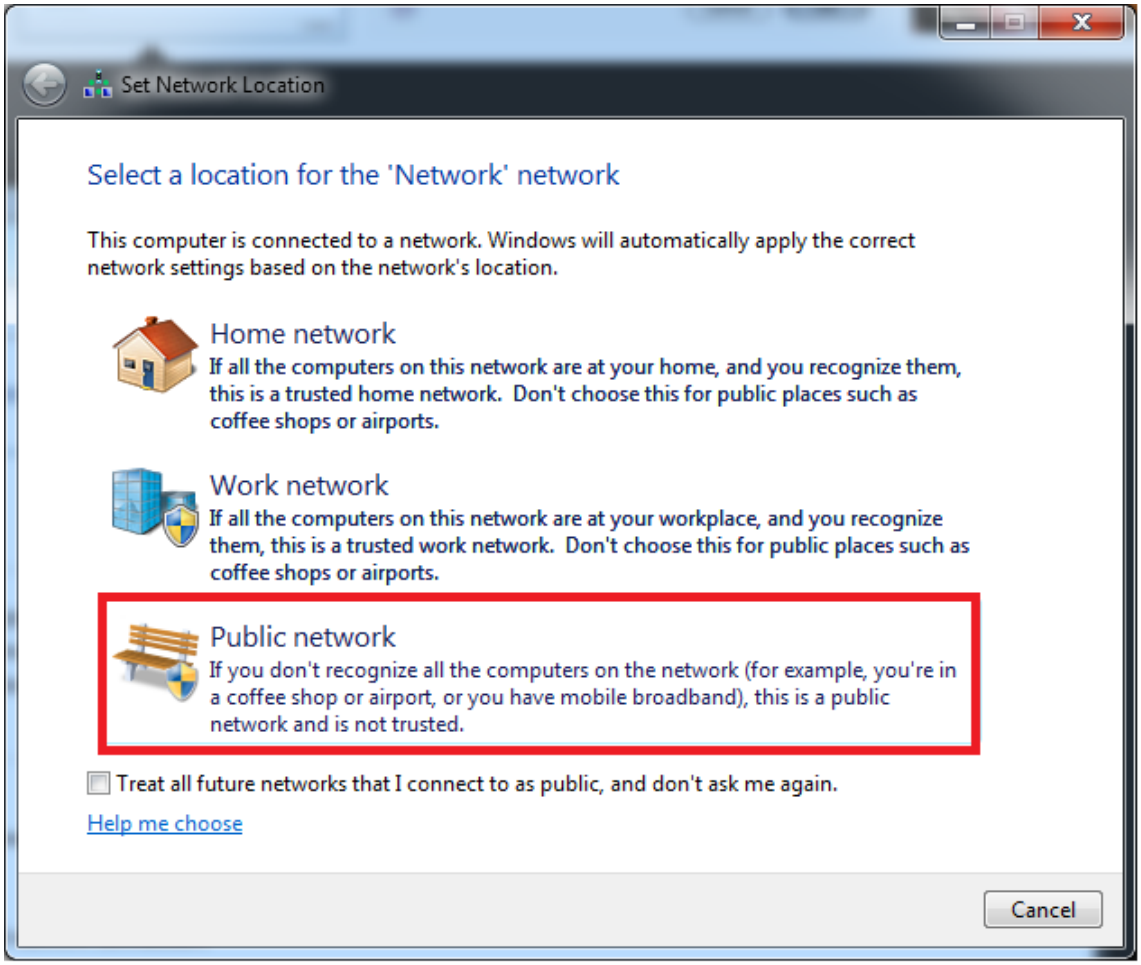


Kuva 5. KeePass-ohjelman hallinta.

Salasanoja voi myös tallentaa selaimiin, mutta ne eivät ole suojattuja, tai suojaukset ovat helposti kierrettävissä. Firefox on tässä poikkeus. Siihen voi asettaa Master-salasanan, jonka jälkeen salasanat avautuvat. Tämä ei ole oletuksena käytössä, joten käyttäjän tulee itse asettaa se.

11 INTERNET-YHTEYS

Julkisiin verkkoihin yhdistettäessä on tärkeää käyttää ”julkista verkkoa” (Kuva 6), ettei jaa omia jakojaan muille sen verkon käyttäjille. Näihin tietoihin kuuluvat sen hetkisellä tietokoneella jaetut tiedostot. Myöskään internetin kautta tehtäviä kirjautumisia ja suojaamattomia ostoja tulisi välttää, sillä joku voi salakuunnella taustalla.



Kuva 6. Liittyminen julkiseen verkkoon.

11.1 WLAN

Langattoman lähiverkon rakentaminen on nykyään halpaa, minkä vuoksi se on erittäin suosittu yhteydenmuoto. Langattomuus tuo kuitenkin turvallisuusriskin, jos ei tiedä, miten yhteys tulisi suojata.

Langattoman verkon huonona puolena voidaankin pitää sen turvattomuutta. Kuka tahansa voi ainakin löytää langattomat verkot, mutta verkon salasanan löytäminen voi tuottaa hankaluuksia.

Suojaus aloitetaan verkon nimestä, eli SSID:stä. Sen ei tulisi ilmoittaa, että se on juuri kyseisen käyttäjän verkko, sillä nimi voi antaa mahdollisuuden kohdennettuihin hyökkäyksiin.

Ensimmäinen langattoman verkon suojaus oli WEP-salaus (Wired Equivalent Privacy). Se kuitenkin havaitiin nopeasti haavoittuvaiseksi. Nykykoneilla WEP-salaus murtuu minuuteissa, eikä salasanan pituudella ole väliä. Pian tähän kehitettiin uusi suojaus nimeltään WPA.

WPA2-salaus on tällä hetkellä paras ja uusin suojaustyyppi. On löydetty ainoastaan yksi tunnettu hyökkäyskeino nimeltään Hole196. Hole196 vaatii, että se tietää jo verkon salauksen. Tämän jälkeen Hole196 mahdollistaa salatun liikenteen kaappaamisen Man-in-the-middle-hyökkäyksen tavoin osapuolten väliin tietoliikenteen välittäjäksi (Airtightnetwork 2014).

Paras murtautumiskeino WPA2-salausta vastaan tällä hetkellä on käyttää sanakirjahyökkäystä tai brute force-tekniikkaa. Hyvään salasanaan löytyy apua kohdasta Salasanat. Uusimmat langattoman verkon laitteet sisältävät valmiiksi WPA2-suojauksen.

11.2 Nettitikku

Nettitikuissa ei usein ole laitepalomuuria. Tästä syystä nettitikkuja käytävissä tietokoneissa tulee olla palomuuri kunnossa. Tähän löytyy apuja reitittimistä, jotka tukevat nettitikkuja.

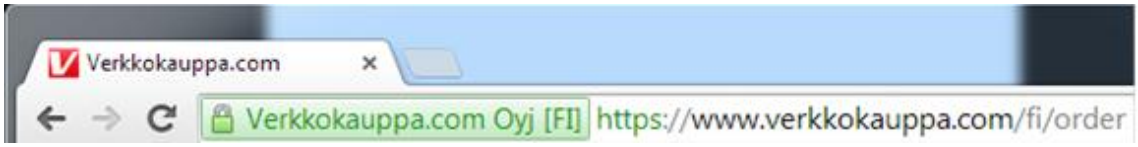
Nettitikun PIN-koodi tulee vaihtaa oletuksesta muuhun, sillä jos nettitikku hukkuu, nettitikun SIM-kortilla voidaan soittaa puheluita ja lähettää teksitiviestejä.

Nettitikulla ei ole tarkoituskaan soittaa puheluita, joten liittymään kannattaa laittaa puheluiden estot päälle siltä varalta, että laite hukkuu.

12 INTERNET-OSTOT

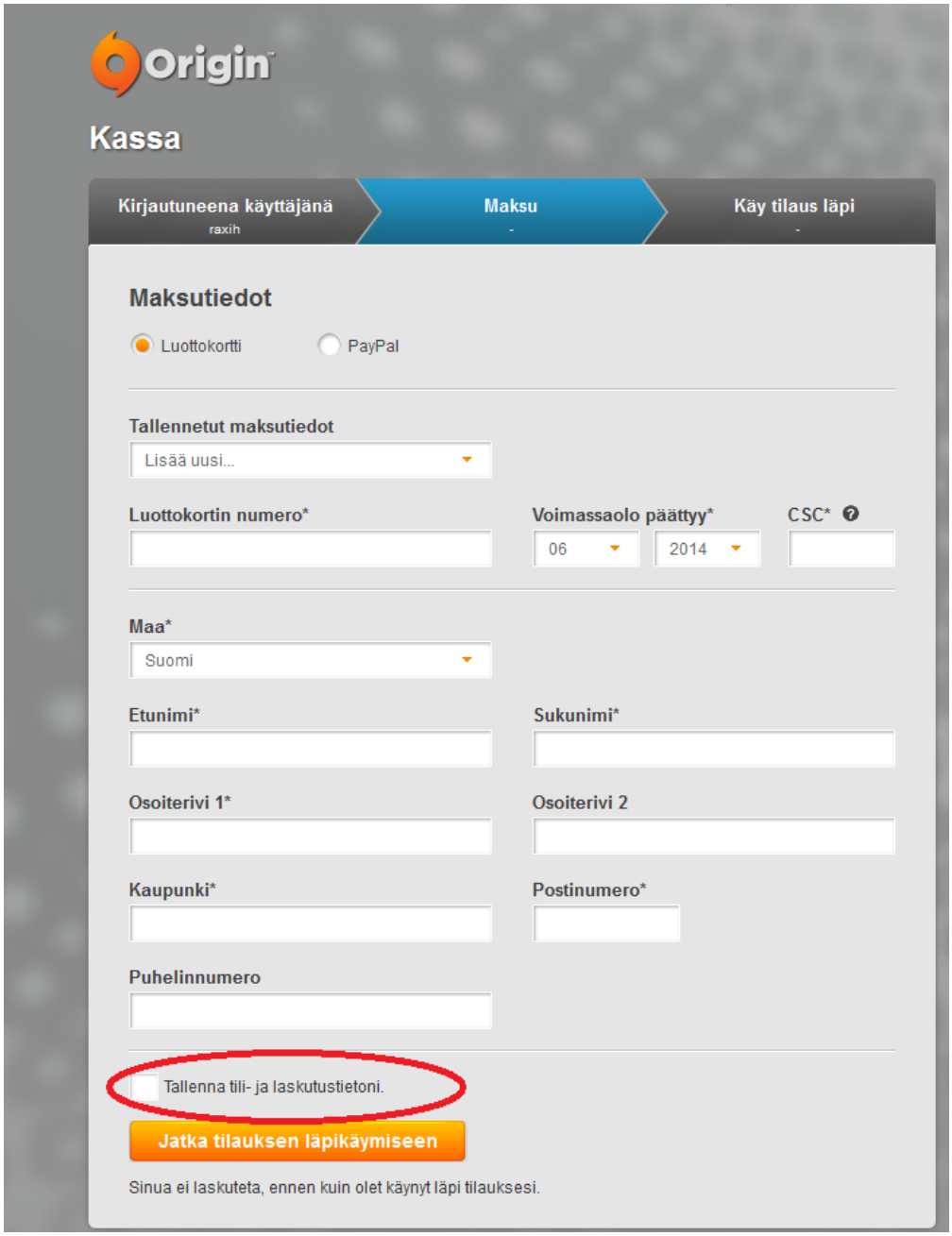
Tietoturvallisesti internetin ostokset tulisi aina tehdä luotetuista verkoista, kuten kotona. Julkisissa WLAN-verkoissa asioinnin voi tallentaa jokin kolmas osapuoli.

HTTPS-protokolla salaa tiedot ennen lähettämistä, mikä tekee siitä turvallisemman vaihtoehdon verkkokaupalle. Verkkosivuilla, joilta ostoksia tehdään, tulisi ehdottomasti olla tämä käytössä. Suojauksen olemassaolon näkee kuvassa 7 esiintyvän linkin alussa olevasta HTTPS-protokollasta.



Kuva 7. Verkkokaupan HTTPS –suojaus.

Tietokoneen kautta tehdyissä ostoissa on hyvä ennen maksun hyväksymistä tarkistaa, ettei tallenna tietojaan, kuten laskutus- tai tilitietoja (Kuva 8). Tietojen tallennus nopeuttaa seuraavaa maksukertaa. Jos rikolliset pääsevät uhrin koneelle onnistuneella verkkopalveluun murtautumisella tai pääsevät kirjautumaan tiliin, voivat omat maksukorttitiedot olla vaarassa.



Kuva 8. Origin-verkkokaupan maksutietojen näkymä.

Verkkokauppoihin voi rekisteröityä, mutta sitä ei aina tarvita. Tietosuojan kannalta rekisteröintiä ei kannata tehdä, etteivät omat tiedot tallennu palvelun ylläpitäjälle.

13 MUUT LAITTEET

Puhelimet ja tabletit sisältävät nykyään paljon henkilökohtaisia tietoja, kuten sähköpostia, kuvia ja luottamuksellisia viestejä. Tästä syystä laitteissa tulee olla tietoturva-asioiden kunnossa.

Kotitalouden laitteissa yleistyvät internetin palvelut, kuten esimerkiksi televisioissa ja jopa jääkaapeissa. Proofpointin tutkimuksessa on selvinnyt, että jopa jääkaappi on lähettänyt roskapostia. Laitteisiin oltiin päästy käsiksi oletussalasanalla. (Proofpoint 2014.)

13.1 PIN-koodit

Uusien laitteiden oletussalasanat tulee aina vaihtaa ensimmäisenä, jotta tietoturva säilyy. Puhelinten ja tablettien suojakoodit estävät ulkopuolisen henkilön pääsyn kyseisiin laitteisiin.

PIN-koodi (Personal Identification Number) tulisi vaihtaa oletuksesta johonkin muuhun. Yleisimmät koodit ovat ”0000”, tai ”1234”. PIN-koodi suojaa liittymää, ei puhelinta. Mikäli PIN-koodin kirjoittaa 3 kertaa väärin, kysyy puhelin PUK-koodia. PUK-koodin voi saada liittymän operaattorilta soittamalla ja todistamalla henkilöllisyytensä, minkä voi myös tehdä onnistuneen identiteettivarkauden suorittanut taho.

13.2 Hukkunut laite

Uusimmissa laitteissa on usein toimintoina ”paikanna puhelin” tai ”lähetä merkkiääni” sekä mahdollisuus etätyhjentää puhelin. Jos laitteessa ei ole näitä, on ne ladattavissa valmistajan kaupasta. Puhelimissa on myös mahdollisuus lähettää puhelimen näyttöön yhteystiedot, joiden avulla puhelimen löytäjä voi soittaa omistajalle ja kertoa, missä puhelin nyt on.

14 POHDINTA

Tämän työn tavoitteena oli perehtyä eri tapoihin suojata yksityisyyttä ja tietoturvaa. Jouduin pohtimaan aihetta paljon, sillä aihe on erittäin laaja. Siihen olisi voinut sisällyttää myös muita asioita, kuten kaikki huijareiden mahdolliset huijaustavat tai enemmän tietoa eri laitteiden suojauksista, mutta silloin työstä olisi helposti tullut erittäin pitkä. Onnistuin mielestäni hyvin rajaamaan aihetta ja kertomaan monesta aiheeseen liittyvästä olennaisesta osasta.

Opinnäytetyötä tehdessäni huomasin kuinka monin eri keinoin rikolliset hyödyntävät eri menetelmiä saadakseen käyttäjien tietoja haltuunsa. Yleensä rikolliset ovat siellä, missä on paljon käyttäjiä. Käyttäjien valppaudella pystytään estämään monia näistä. Hyvänä esimerkkinä tästä on roskapostit, sillä usein ne ovat huonosti kirjoitettuja.

Tietoturvasta huolehtiminen on jatkuvaa, sillä tekniikka kehittyy kovaa vauhtia ja uusia huijaustapoja löytyy aina silloin tällöin. Koen, että opinnäytetyöni kohderyhmänä ovat nykyajan laitteiden peruskäyttäjät. Mielestäni peruskäyttäjät tarvitsevat lisää tietoa välttyäkseen esimerkiksi viruksilta tai identiteettivarkauksilta.

Työni kautta olen saanut hyvän pohjan, jonka takia tietoturva on minulle tärkeä ja mielenkiintoinen aiheena. Tietoa etsiessäni omat tietoni kehittyivät ja koen saaneeni hyötyä tulevaisuutta varten työelämään.

LÄHTEET

Adware 2014. Wikipedia. Viitattu 1.6.2014
http://en.wikipedia.org/wiki/Adware.

Airtightnetwork 2014. WPA2 Hole196. Viitattu 2.6.2014
http://www.airtightnetworks.com/WPA2-Hole196.

BBC 2010. What is an internet worm?. Viitattu 1.6.2014
http://www.bbc.co.uk/webwise/guides/internet-worms.

BBC 2012. What is spyware?. Viitattu 1.6.2014
http://www.bbc.co.uk/webwise/guides/about-spyware.

Cisco 2014. Annual Security Report. Viitattu 22.5.2014
https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

Computer Virus 2014. Wikipedia. Viitattu 21.5.2014
http://en.wikipedia.org/wiki/Computer_virus.

Dataprotectioncenter 2011. Trends: From Phishing to “Man-in-the-Middle” Phishing. Viitattu 4.5.2014
http://www.dataprotectioncenter.com/antivirus/f-secure/trends-from-phishing-to-man-in-the-middle-phishing/.

Domnik 2011. Suomalaisten sata yleisintä salasanaa. Viitattu 20.4.2014
http://aiheet.domnik.net/ai-2011/11/100-yleisinta-salasanaa.

F-Secure Labs 2013. Threat Report H1 2013. Viitattu 25.8.2014
http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf.

Kaspersky 2014. What is a Trojan Virus?. Viitattu 1.6.2014
http://usa.kaspersky.com/internet-security-center/threats/trojans.

Lehto, E. & Kjellberg, H. 2011. Krp tutkii Suomen suurinta henkilötieto-vuotoa, tuhansien henkilötunnukset netissä. Helsingin Sanomat 5.11.2011. Viitattu 19.8.2014
http://www.hs.fi/kotimaa/a1305548766402.

Microsoft Malware Protection Center 2012. Another way Microsoft is disrupting the malware ecosystem . Viitattu 20.3.2014
http://blogs.technet.com/b/mmpc/archive/2012/11/29/another-way-microsoft-is-disrupting-the-malware-ecosystem.aspx.

Norton Identity Theft 2014. Identiteettivarkauden välttäminen. Viitattu 2.6.2014
http://fi.norton.com/identity-theft-primer/article.

PlayStation Network katkos 2014. Wikipedia. Viitattu 20.5.2014
http://fi.wikipedia.org/wiki/PlayStation_Network_-katkos.

Proofpoint 2014. Proofpoint Uncovers Internet of Things (IoT) Cyberattack . Viitattu 1.6.2014
http://www.proofpoint.com/about-us/press-releases/01162014.php.

The Telegraph 2014. Cybercriminals already targeting Windows XP . Viitattu 22.5.2014
http://www.telegraph.co.uk/technology/internet-security/10761002/Cybercriminals-already-targeting-Windows-XP.html.

Tietokonevirus 2013. Wikipedia. Viitattu 1.6.2014
http://fi.wikipedia.org/wiki/Tietokonevirus.

Viestintävirasto 2013. Ohjeita viestinnän suojaamiseen. Viitattu 1.5.2014
https://www.viestintavirasto.fi/ohjausjavalvonta/ohjeettulkinnatsuosituksetjaselvitykset/ohjeidentulkintojensuositustenjaselvitystenasiakirjat/ohjeitaviestinnansuojaamiseen.html

Zdnet 2014. Windows XP: Microsoft can't wash its hands of the security problem so easily. Viitattu 2.6.2014
http://www.zdnet.com/windows-xp-microsoft-cant-wash-its-hands-of-the-security-problem-so-easily-7000029025/.

Zsecurity 2009. Rootkit: Definition, Prevention and Removal. Viitattu 1.6.2014
http://www.zsecurity.com/articles-rootkits.php.

Åström-Kupsanen, M . 2012. Identiteettivarkaus sekoittaa elämän. Yle 2.2.2012. Viitattu 15.4.2014 http://yle.fi/aihe/artikkeli/2012/02/02/identiteettivarkaus-sekoittaa-elaman.

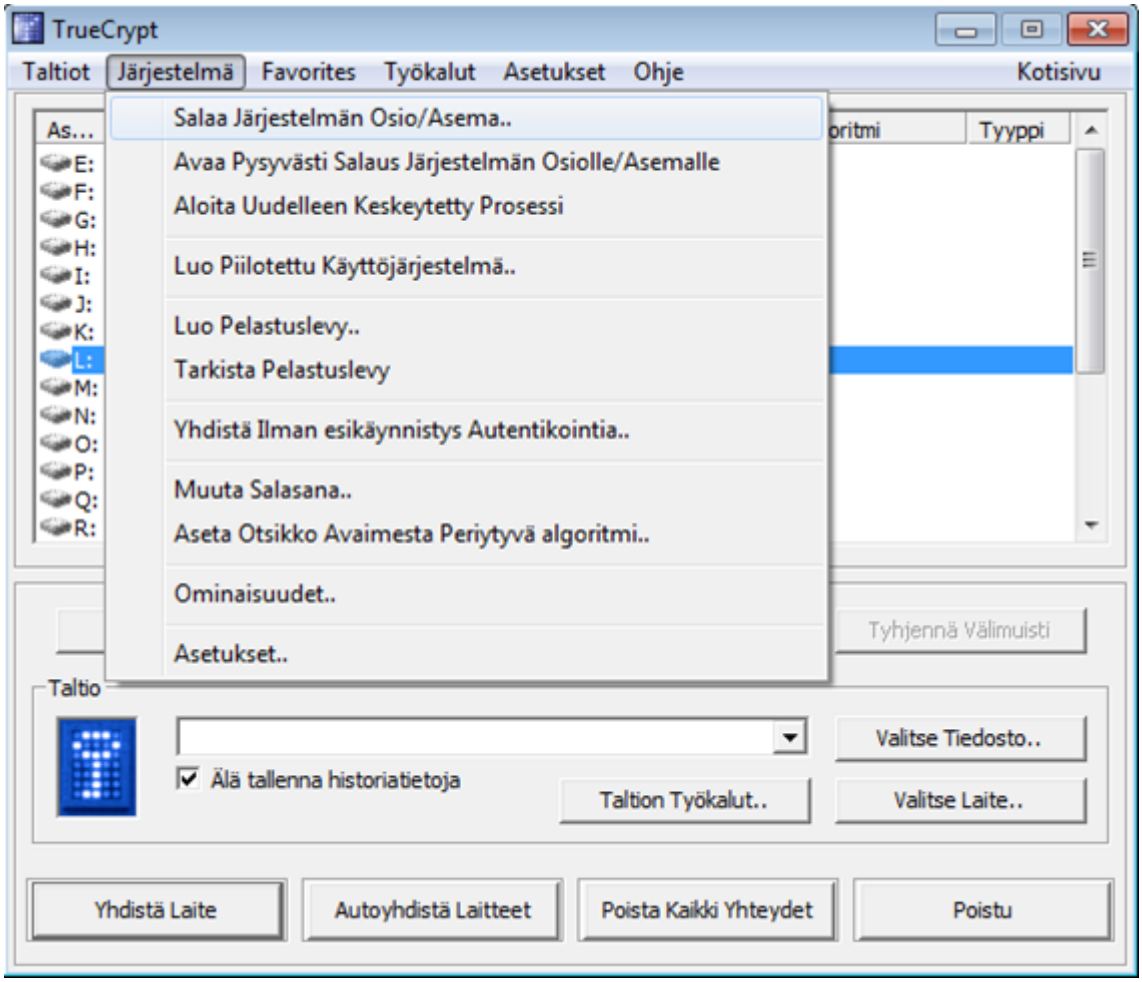
LIITE 1. YLEISIÄ VINKKEJÄ

- Vaihda aina salasanat oletuksista pois.
- Älä pidä samaa salasanaa monessa eri paikassa.
- Uusien ohjelmien asennuksissa tulee olla tarkkana. Jotkin niistä sisällyttävät muita ohjelmia, kuten työkalurivejä tai jopa haitallisia ohjelmia. Tutki siis tarkkaan, mitä asennuksessa lukee ennen kuin jatkat asennusta. Jos epäilet uutta ohjelmaa, etsi siitä tietoa esimerkiksi googlesta.
- Pidä ohjelmistot aina päivitettyinä. Useat haittaohjelmat leviävät päivittämättömien ohjelmien kautta.
- Yksityisyydestään huolehtiville on ohjelmia, joiden avulla voi pysyä nimettömänä internetissä. TOR-ohjelman avulla voi selata nettiä anonyymisti, eli nimettömänä. TOR-selaimen asennus onnistuu myös Android-alustoille.
- Ccleaner on luotettava ja ilmainen apuohjelma, jonka avulla pystyt siivoamaan tietokoneesi ylimääräisistä tiedostoista kuten evästeistä, tai puhdistamaan Windowsin rekisterin virheistä.
- Poista ylimääräiset ohjelmat tietokonelta, joita et tarvitse. Java voi olla yksi näistä.
- Muista aina kirjautua ulos palveluista, kun et enää niitä käytä.
- Seuraa tietoturva-aiheisia sivuja. Cert.fi (www.cert.fi) on suomen viestintäviraston kyberturvallisuuskeskus, josta saa nopeasti tietoa uusista tietomurroista, haavoittuvuuksista, varoituksista sekä huijauksista.
- Jos jokin mainos kuulostaa liian hyvältä ollakseen totta, todennäköisesti se on juuri sitä.
- Lataa mobiilisovelluksia vain valmistajan omilta sivuilta. Tutki tarkkaan mitä oikeuksia ohjelma vaatii ennen asentamista.
- Älä koskaan anna vanhaa tietokonettasi pois ennen kuin olet tyhjentänyt turvallisesti kiintolevyn sisällön. Pelkkä alustaminen ei riitä

Liite 2. Kiintolevyn salaaminen Truecrypt-ohjelman avulla

Viimeisin vakaa ohjelmaversio Truecryptistä on kirjoittamisen aikaan versio 7.1a.

Sekä yrityksillä että yksityisillä henkilöillä voi olla tiedostoja tai dokumentteja, joita ei halua ulkopuolisten näkevän. Windowsin suojaus ainoastaan Windowsin salasanalla ei ole riittävä suojaus, kuten aiemmin huomattiin. TrueCrypt on avoimen lähdekoodin ohjelma, jonka avulla voi suojata kiintolevyt, osion tai esimerkiksi muistitikun salasanalla. Salasana kannattaa suojata hyvin ja suosittelen käyttämään tässä opinnäytetyössä olevaa vahvan salasanan ohjeita. Ainoa miinus kiintolevyn salauksella on käyttöjärjestelmän hieman hidastunut toiminta. Salaukseen tarvitaan yksi tyhjä CD/DVD-levy. Kuvassa näet TrueCrypt salauksen aloituksen.



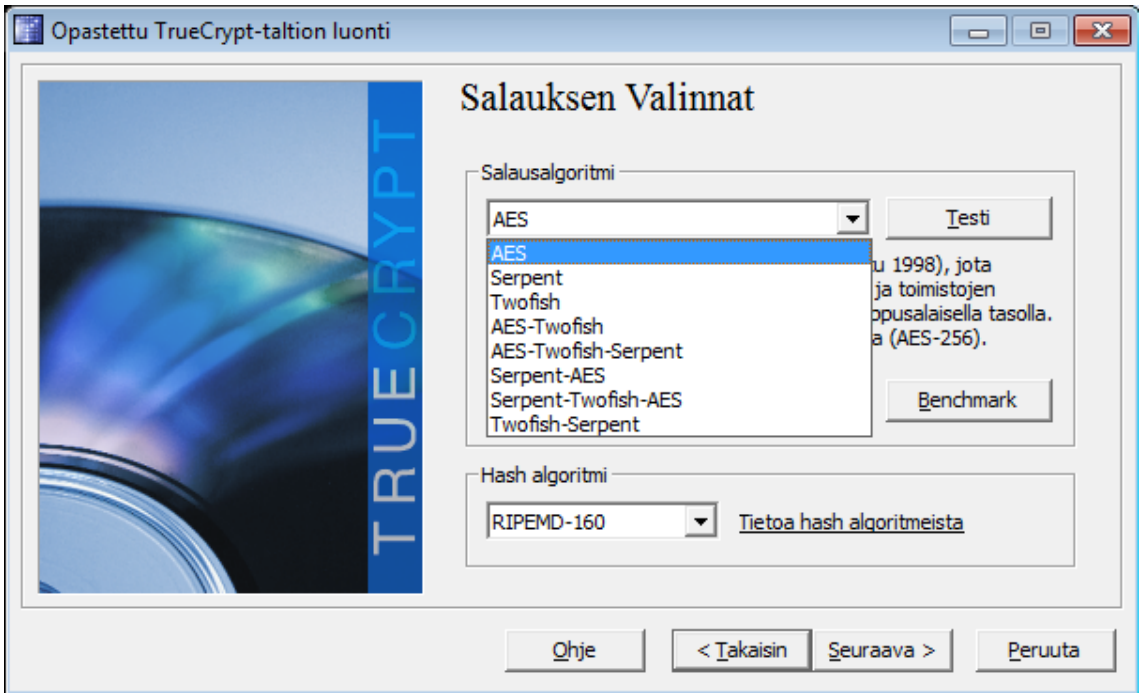
Kiintolevyn salaus aloitetaan käynnistämällä TrueCrypt ja valitsemalla Järjestelmä-valikosta ”Salaa järjestelmän osio/asema”. Seuraavaksi valitaan järjestelmän salauksen tyyppi, joka voi olla joko normaali tai piilotettu. Tässä esimerkissä valitsen normaalin, koska aikomus on ainoastaan salataan järjestelmä.

Tämän jälkeen TrueCrypt kysyy salauksen aluetta. Alueita on valittavana joko ainoastaan Windowsin järjestelmä, tai koko asema. Valitse koko järjestelmä.

Seuraavassa vaiheessa ohjelma kysyy salataanko ”isäntä suojattu alue”. Tämä tarkoittaa sitä, että salataanko kiintolevy kokonaisuudessaan, vai jätetäänkö loppuun alue, johon jotkin ohjelmat voivat kirjoittavat ja lukevat tietoa. Mikäli vastaa kyllä, voi tulla ongelmia esimerkiksi järjestelmän toipumisessa tai RAID-järjestelmissä. Tässä esimerkissä valitaan ”Kyllä”. Tämän jälkeen Truecrypt tunnistaa kiintolevyn piilotetut sektorit,

Nyt ohjelma kysyy käyttöjärjestelmän numeroa. Valitaan Single-boot, koska ainoastaan yksi käyttöjärjestelmä on asennettuna.

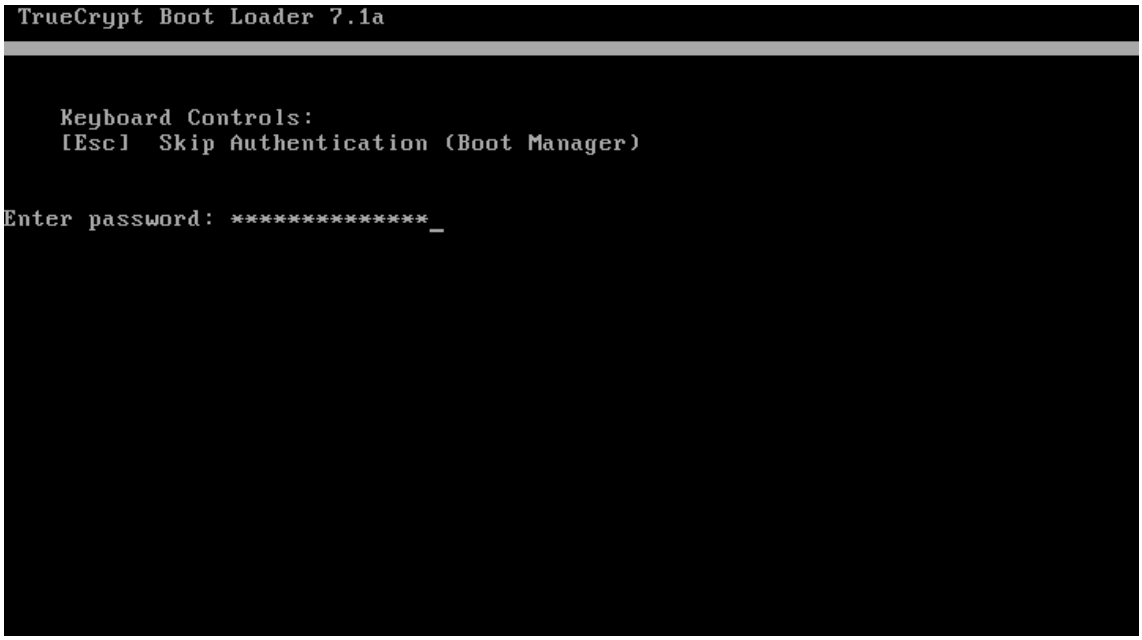
Salauksen valinnassa on monta eri eri salausalgoritmia valittavana. Näistä voi valita itselleen mieleisen salaustyypin. Salaustyypit näet alla olevasta kuvasta. Nopeustesti kannattaa suorittaa, jotta näkee kuinka paljon salaus hidastaa salatun järjestelmän toimintaa. Kun salaus on valittu, tulee asettaa salasana. Salasanan asetussivu muistuttaa hyvästä salasanasta. Jos salasana on alle 20 merkkiä pitkä, ohjelma varoittaa heikosta suojauksesta.



Tämän jälkeen ohjelma kerää satunnaista dataa, tarkoittaen mitä kauemmin hiirtä liikuttaa ikkunassa, sitä paremman suojan saa. Suositus on vähintään muutaman minuutin. Seuraavaa painamalla Truecrypt ilmoittaa, että se on luonut sekä otsikko- että pääavaimen.

Tee pelastuslevy. Siihen tarvitaan tyhjä CD/DVD-levy. Tämän jälkeen on mahdollisuus valita salattavaksi tyhjennystila. Valitse ei mitään.

Truecrypt haluaa nyt testata, että kaikki toimii oikein. Testi käynnistää tietokoneen uudelleen. Käynnistäessä konetta tulee alla olevan kuvan mukainen alkuruutu. Tähän laitetaan asetettu salasana, jotta asetusten oikeus tarkistetaan.



Tietokoneen käynnistys kiintolevyn salauksen jälkeen. Jos Truecrypt huomasi kaiken toimivan hyvin, pääsee salaamaan järjestelmän.

Yksittäisten tiedostojen salaukseen AxCrypt on suositeltu ohjelma.

Liite 3. Tiedostojen palautus

Tiedostojen poistosta luullaan, että kun on roskakorista poistanut tiedostot, ne ovat pysyvästi poissa. Todellisuudessa tiedostot ovat tällöin ainoastaan näkymättömissä. Käyttöjärjestelmä poistaa silloin ainoastaan poistetun tiedoston viitteen tiedostojärjestelmästä. Tieto jää levylle kunnes toinen tiedosto on luotu vanhan päälle.

Tiedostojen palautus on yllättävän helppoa esimerkiksi Recuva-ohjelman avulla.

Testiksi tein kuvan nimeltään Kuva.jpg, jonka aion poistaa normaalilla tavalla ja palauttaa sen. Kuvan poistamisen jälkeen ja roskakorin tyhjennyksen jälkeen käynnistetään Recuva.

Kun ohjelma on avattu, ohjelma kysyy mitä tiedostoa etsitään ja mistä. Haku kestää noin 10 sekuntia ja ohjelma löytää kuvan, jonka poistettiin.

Liite 4. Tiedostojen turvallinen poisto

Jotta kuvan voisi poistaa niin, ettei sitä pysty ainakaan helposti palauttaa, pitää kirjoittaa kiintolevyn poistetun tiedon päälle uutta satunnaista tietoa. Yksi avoimen lähdekoodin ohjelma tähän on Eraser-niminen ohjelma. Eraser kirjoittaa useaan kertaan satunnaista kuviota poistettavan tiedoston päälle, mikä tekee tiedoston palauttamisesta erittäin vaikeaa. Ohjelmassa on mahdollisuus valita myös eri poistometodeja. Eraser-ohjelmalla tiedoston poistaminen näkyy alla olevasta kuvasta.