LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Henkilöstön tietoturvakoulutus EU:n tietosuojauudistuksen yhteydessä

Risto Hämäläinen

2018 Laurea

Laurea-ammattikorkeakoulu

Henkilöstön tietoturvakoulutus EU:n tietosuojauudistuksen yhteydessä

Risto Hämäläinen
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Toukokuu, 2018

Laurea-ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Tradenomi (AMK)

Hämäläinen Risto

Tiivistelmä

Henkilöstön tietoturvakoulutus EU:n tietosuojauudistuksen yhteydessä

Vuosi 2018 Sivumäärä 30

Tämän opinnäytetyön tarkoituksena oli luoda tietoturvakoulutus, joka vähentäisi henkilöstöön liittyviä tietoturvauhkia. Henkilöstön koulutus on osa prosessia, jolla voidaan osoittaa, että yritys on ottanut toiminnassaan huomioon EU:n tietosuoja-asetuksen vaatimukset. Opinnäytetyön toimenantaja oli Smartum Oy.

Viitekehyksenä koulutuksessa käytettiin toimintatutkimusta. Toimintatutkimus on tutkimuksen suuntaus, missä tutkimuksen tekijä pyrkii vaikuttamaan suoraan organisaation toimintaan. Opinnäytetyön tietoperusta sisälsi kirjallisuutta liittyen tietoturvaohjeistuksiin, tietosuoja-asetukseen sekä toimintatutkimukseen.

Tietoturvakoulutus pidettiin koko henkilöstölle luentomuotoisena esityksenä. Koulutuksen materiaali löytyy yrityksen tietoturvasivuilta. Koulutusmateriaalin sisältö oli suunniteltu niin, ettei sen ymmärtämiseksi tarvitse minkäänlaista teknistä ymmärtämistä.

Toimenantajan antama palaute oli positiivista. Koulutuksen teemat oli valittu hyvin ja esitys eteni loogisesti ja oli kuulijan kannalta selkeästi ymmärrettävässä muodossa. Koulutuksen konkreettista vaikutusta oli kuitenkin vaikeaa mitata. Tulevaisuudessa koulutustilaisuuksia varten voitaisiin luoda testi tai kysely, jolla koulutuksen vaikutuksesta saataisiin parempi kuva.

Asiasanat: Tietoturva, GDPR, Tietosuoja-asetus, Tietoturvakoulutus, Tietosuoja

Laurea University of Applied Sciences **Abstract**
Degree Programme in Business Information Technology
Bachelor's Thesis

Hämäläinen Risto

GDPR and an Information Security Training Program for Personnel

Year 2018 Pages 30

The purpose of this thesis was to produce an information security training program for the personnel of Smartum Oy. The objective was to reduce the threats that could be caused by the personnel of the company. Training the personnel was a part of the process; with it the company can show that it has taken into account the required actions demanded by EU's general data protection regulation.

The framework used for this thesis was action research. Action research is usually done by actively participating in the situation that needs a change, while simultaneously doing research. The knowledge base used for this thesis consists mainly of literature on information security, general data protection regulation and action research.

The information security training program was held to the whole organisations personnel as a lecture. The material produced for the lecture can be found on the organisations intranet. The material for the lecture was written in a way that in can be understood without any kind of technical background.

The feedback given by the employer was positive. The themes chosen for the lecture were chosen well and the presentation was easy to follow. It was hard to evaluate the impact that the lectures had without any reference material. For the future lectures, it could be useful to create a test or a survey, that the employees could take after the lecture to measure the real influence.

Keywords: GDPR, Data Protection, Information Security, Computer Security

Sisällys

1 Johdanto

EU:n tietosuojauudistus on asetus, jota alettiin soveltamaan 24.5.2016 alkaen kaikissa EU:n jäsenmaissa. Asetuksen tuomat sanktiot tulevat voimaan 25.5.2018. Tietosuoja-asetusta sovelletaan kaikkeen henkilötietoihin liittyvään käsittelyyn. Asetuksen rikkomisesta voi seurata esimerkiksi sakkoja tai henkilötietojen käsittelykielto. Uusi asetus velvoittaa henkilötietoja käsittelevän yrityksen pystyvän konkreettisesti osoittamaan, että uusi tietosuojasäädös on otettu huomioon yrityksen toiminnassa (Tietosuoja.fi 2015).

Tämän opinnäytetyön tavoitteena on parantaa henkilöstön tietoturvatuntemuksen tasoa ja vähentää henkilöstöön liittyviä tietoturvauhkia. Koulutus on osa prosessia, jolla voidaan osoittaa yrityksen tietoturvan olevan riittävällä tasolla tietosuojauudistusta varten.

Tietoturvakoulutuksen tarve huomattiin yrityksen tietoturvaryhmän kokouksessa, missä käytiin läpi asioita, joita täytyy tehdä tietosuoja-asetuksen noudattamista varten. Aikaisemmat tietoturvakoulutukset eivät olleet kattanut kaikkia EU:n tietosuojauudistuksen tuomia vaatimuksia, koska nämä oli pidetty ennen uuden tietosuoja-asetuksen astumista voimaan.

Tietoturvakoulutus pidettiin koko yrityksen henkilökunnalle, ja sitä varten luotu materiaali löytyy yrityksen tietoturvasivuilta heidän intranetistä. Materiaali on kirjoitettu niin, että sitä pystytään hyödyntämään ilman erillistä koulutusta. Koulutus kuitenkin toi lisäarvoa kysymysten kautta ja sen avulla pystyttiin käsittelemään asioita syvemmin.

1.1 Taustaa

Työnantajana on Smartum Oy, joka on suomalainen 1995 perustettu perheyritys. Sen liiketoiminta on kehittää hyvinvointipalveluja työelämää varten. Smartumilla on yli 13 000 työnantaja-asiakasta, joissa on töissä noin miljoona työntekijää. Yrityksen tuotteita ovat muun muassa Smartum Lounasseteli ja saldo, Smartum Työmatkasaldo, Smartum Liikunta- ja kulttuuri seteli sekä Smartum liikuntaseteli.

Olen toiminut Smartumilla kiireapulaisena vuodesta 2012 ja suoritin keväällä 2017 viiden kuukauden työharjoitteluni siellä. Työharjoittelussa tehtäväni oli toimia IT lähitukena sen ajan, kuin varsinainen tuki oli kesälomalla. Tämän jälkeen työtehtäväni oli osallistua yrityksen suorittamaan GDPR eli uuden tietosuoja-asetuksen vaatimaan auditointiin. Tämä auditointi koski pääosin yrityksen järjestelmiä ja teknistä tietoturvaa.

Ollessani työharjoittelussa päätin kysyä olisiko heillä aiheita tarjolla opinnäytetyötä varten. Tästä lähti liikkeelle henkilöstöön liittyvä tietoturva uhkien vähentäminen. Ensimmäinen ehdotus opinnäytetyöksi oli ohjeistus henkilötietojen käsittelijöille tietosuojauudistusta varten. Lopulta kehityskohteita tutkiessa päädyttiin siihen, että opinnäyteyön aiheeksi tulisi yleinen

tietoturvakoulutus koko yrityksen henkilöstölle, jonka tarkoituksena oli vähentää henkilöstöön liittyviä tietoturvauhkia ottamalla huomioon myös EU:n tietosuojauudistus.

2 Tietoperusta

Tämän opinnäytetyön tietoperusta voidaan jakaa kolmeen eri osa-alueeseen: tietoturvaan, tietosuojaan ja koulutukseen. Tietoturvan ja tietoturvan asiakokonaisuudet menevät usein sekaisin. Tietoturvaa usein pidetään ylätason käsitteenä, johon kuuluu tietosuoja. Tietosuoja kuitenkin tarkoittaa yksilön luottamuksen ja yksityisyyden suojaamista. EU:n tietosuojauudistus kuitenkin tuo uusia velvoitteita suojaamaan yksilön oikeudet ja vapaudet laajasti, ja se käsittelee laajempaa kokonaisuutta kuin vain yksityisyyden suojaa. Tietoturvalla tarkoitetaan niitä hallinnollisia ja teknisiä toimenpiteitä joilla pyritään tietosuojan toteutumisen (OpiTietosuojaa.fi 2016).

2.1 Tietoturva

Tietoturva tarkoittaa niitä teknisiä ja hallinnollisia toimenpiteitä, joilla varmistetaan rekisteröidyn oikeuksien toteutuminen, järjestelmien käytettävyys sekä tietojen luottamuksellisuus ja eheys (Tietosuoja.fi 2013).

Käytettävyydellä tarkoitetaan sitä, että järjestelmissä olevat tiedot ovat aina saatavilla, kun niitä tarvitaan. Luottamuksellisuudella varmistetaan se, että tietoa voi käsitellä vain henkilöt joilla on siihen oikeus. Eheyden ylläpitämisellä pidetään huolta siitä, ettei tieto muutu vahingossa tai hyökkäyksessä. Jos muutos tapahtuu, se täytyy kuitenkin havaita. Eheys voidaan myös määritellä paikkansapitävyydeksi ja loogisuudeksi (Metivier 2017).

Hallinnollisella tietoturvalla tarkoitetaan keinoja, kuten organisaatiojärjestelyt, henkilöstön ohjeistus, koulutus ja valvonta sekä tehtävien ja vastuiden määrittely. Henkilökunnan tulisi olla vahvin lenkki tietoturvallisuudessa, minkä takia koulutus ja tiedotus ovat oleellisia tehtäviä (VAHTI 2009).

Tietoperustana opinnäytetyössä on käytetty erilaisia tietoturvakokoelmia, kuten valtiovarainministeriön VAHTI-toiminnan dokumentteja ja Tietosuoja.fi sivuston tarjoamaa materiaalia. VAHTI-toiminta on luonut useita tietoturvaohjeistuksia. Tässä opinnäytetyössä on käytetty apuna varsinkin heidän vuonna 2006 kirjoittamaa henkilöstön tietoturvaohjetta. Koulutus materiaalia kasatessa on myös tutustuttu Itäsuomen Yliopiston julkaisemaan tietoturvaohjeistukseen henkilöstölle.

Yritystä vaativaa yksilöintiä varten on tutustuttu aikaisempiin tietoturvaohjeistuksiin. Myös aikaisemmasta työkokemuksesta yrityksessä oli hyötyä, sillä yrityksen kulttuurista oli jo hyvä kuva.

2.2 Tietosuoja

”Tietosuojaan kuuluu ihmisten yksityiselämän suoja ja muut sitä turvaavat oikeudet henkilötietoja käsitellessä.” (Tietosuoja.fi 2013.) Tämä tarkoittaa sitä, että henkilötietoja tulee käsitellä oikeaoppisesti ja niitä tulee suojata luvattomalta käytöltä ja käsittelyltä. Voidaan sanoa, että tietosuoja on perustuslailla perusoikeutena turvattua niin sanotusti tiedollista kotirauhaa. Ihmisillä on siis peruslain mukaisesti oikeus elää elämäänsä ilman oikeudetonta puuttumista siihen. Tietosuojan tarkoituksena on turvata nämä oikeudet. (OpiTietosuojaa.fi 2016.)

Myös tietosuoja-asetuksen vaatimukset on otettu huomioon tietoturvakoulutusta tehdessä. Tietosuoja.fi sivusto tarjoaa ohjeita asetukseen valmistautumista varten. Sieltä löytyvistä dokumenteista sai kuvan siitä, mitä täytyy ottaa huomioon tietosuoja-asetuksen noudattamista varten. Koulutuksessa tietosuoja-asetus tuli esille varsinkin, kun käsiteltiin luottamuksellisten tietojen käsittelyä.

Tietoperustana oli myös aikaisempi kokemus yrityksen GDPR eli EU:n tietosuojauudistukseen liittyvästä teknisestä auditoinnista sekä tutustuminen tähän asetukseen.

2.3 Koulutus

Koulutuksen suunnittelun apuna on käytetty VAHTI 11/2006 Tietoturvakouluttajan opasta. Oppaasta löytyy ohjeita tietoturvan koulutuksen pitämistä varten. Tietoturvakouluttajan opas tarjoaa neuvoja erilaisia koulutustilanteita varten. Siitä löytyvät ohjeistukset auttoivat koulutusmateriaalin selkeyttämisessä, sekä koulutustilanteeseen valmistautumisessa (VAHTI 2006).

Koulutuksesta tulisi saada irti jotain, jonka avulla pystytään uudistamaan työkäytäntöjä sekä kehittämään niitä tulevaisuuden tarpeisiin. Koulutuksen tulisi olla työn kannalta hyödyllinen, ettei se jää käytännölle vieraaksi ja liian teoreettiseksi. Koulutuksen sisältö voidaan tehdä konkreettisemmaksi ottamalla siihen käytännön esimerkkejä (VAHTI 2006).

Koulutustilaisuutta suunnitellessa täytyy ottaa huomioon sille asetetut tavoitteet, kohdeyleisön tietotaito, käytettävissä oleva tila ja aika sekä kouluttajan koulutusmenetelmät. Kouluttajan on itse suunniteltava, paneutuuko tiettyihin asioihin syvemmin vai käykö kerralla useita asioita läpi. Näitä pohdittaessa täytyy ottaa huomioon yleisön määrä, käytettävissä oleva tila ja aika (VAHTI 2006).

Ryhmäkoko vaikuttaa aktiivisuuteen sekä menetelmävalintoihin. Tätä tietoturvakoulutusta varten pidettiin kaksi koulutusta. Ensimmäiseen osallistui alle 10 henkeä ja toiseen yli 30 henkeä. Yli 30 hengen ryhmässä osallistumismahdollisuus on pieni. Tämän takia koulutusmenetelmäksi valittiin luento (VAHTI 2006).

3 Tutkimusmenetelmät

Viitekehyksenä opinnäytetyössä käytettiin toimintatutkimusta. Toimintatutkimus on tutkimuksen suuntaus, jossa pyritään kehittämään organisaatiota tai sen toimintatapoja vaikuttamisen kautta. Toimintatutkimuksessa on keskeistä tutkijan osallistuminen organisaation toimintaan ja hänen mukana olo sen arkipäivässä.

Viitekehyksen tutkimiseen käytettiin muun muassa Baskervillen vuonna 1999 julkaisemaa tutkimusta toimintatutkimuksesta sekä Touko Ekatuon vuonna 2014 Metodix nimiselle verkkosivulle kirjoittamaa artikkelia. Näitä lähteitä käytettiin toimintatutkimukseen tutustumisessa. Niistä oli varsinkin hyötyä opinnäytetyön kirjoittamisessa selkeään muotoon (Ekatuo 2014).

3.1 Toimintatutkimus

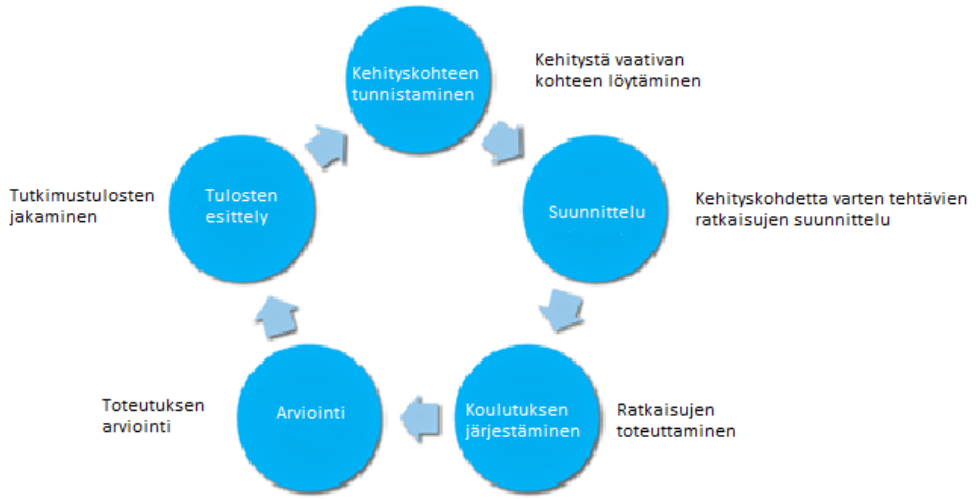
Toimintatutkimuksessa on useita eri suuntauksia. Tässä opinnäytetyössä se esiintyy viisiosaisena kokonaisuutena, joka voidaan toistaa, mikäli kehityskohde sen vaatii.

Tässä opinnäytetyössä on suoritettu yksi iteraatio, mutta mikäli koulutus vaatii myöhemmin päivitystä, voidaan se toteuttaa uudestaan käyttäen toimintatutkimusta tai muita tutkimuksen suuntauksia.

Toimintatutkimus sopi opinnäytetyöhön, sillä sen pyrkimyksenä oli vaikuttaa suoraan yrityksen toimintaan olemalla mukana yrityksen arkipäivässä. Aikaisempi työkokemukseni yrityksessä auttoi minua paremmin ymmärtämään henkilöstön vaatimaa koulutuksen tasoa. Opinnäytetyön tavoitteena oli parantaa henkilöstöön liittyvän tietoturvan tasoa antamalla ohjeistuksia erilaisia tapauksia varten. Opinnäytetyö myös suoritettiin tiiviisti työnantajan kanssa yhteyksissä, joka keskeinen osa toimintatutkimusta (Ekatuo 2014).

3.1.1 Toimintatutkimuksen vaiheet

Tässä opinnäytetyössä on käytetty Richard Baskervillen toimintatutkimuksen mallia. Se koostuu viidestä eri vaiheesta. Tätä työtä varten ne ovat käännetty suomeksi ja tarkoitukseen sopiviksi.



Kuva 1: Tutkimuskehä (Baskerville 1999; Järvinen 2009, muokattu)

Tämän tutkimusmenetelmän ensimmäinen vaihe on tunnistaa organisaatiosta muutosta vaativa kohde. Kehityskohteen tunnistamisvaiheessa tulee ottaa huomioon koko yritys, eikä tehdä ongelmasta pienempää tai yksinkertaisempaa. Tämän vaiheen tarkoituksena on myös saada selville enemmän yrityksestä ja kehitettävästä asiasta.

Seuraavaksi tulee suunnitteluvaihe. Suunnitteluvaiheessa valitaan muutosta tarvitseva kohteet, sekä päämäärä. Tämän jälkeen tehdään suunnitelma päämäärään pääsemiseksi varten, ja aloitetaan tekemään muutoksia sitä kohti. Suunnitteluvaiheen jälkeen aletaan toteuttamaan suunnitelmaa (Baskerville 1999).

Ratkaisujen toteuttamisen jälkeen arvioidaan lopputulos. Arviointivaiheessa selvitetään toimiko teoriapohjalta mietityt ratkaisut ja oliko näistä apua ongelmiin. Mikäli muutos oli onnistunut, täytyy miettiä, oliko tehdyt ratkaisut ainoa syy onnistumiseen. Epäonnistumisten kautta tulee miettiä millaisia muutoksia seuraavaa iteraatiota varten tulisi tehdä (Baskerville 1999).

Viimeinen vaihe tämänkaltaisessa toimintatutkimuksessa on tutkimustulosten jakaminen. Vaikka tämä vaihe tehdään yleensä viimeiseksi, se on usein jatkuva prosessi koko tutkimuksen ajan (Baskerville 1999).

3.2 Benchmarking

Tietoturvakoulutuksen materiaali, joka tuotettiin tietoturvaryhmän kokousten ulkopuolella, toteutettiin pääosin benchmarkingin avulla. Benchmarking eli suomeksi vertailukehittäminen tarkoittaa oman toiminnan vertailua muiden toimintaan nähden, usein parhaaksi nähtyyn käy-

täntöön. Tässä opinnäytetyössä vertailukehitystä käytettiin lähinnä materiaalin sisällön tuottamiseen. Vertailemalla julkisia tietoturvaohjeistuksia ja koulutuksia sai kuvan siitä, mitä muiden tekemät koulutukset sisältävät. Näistä otettiin yritykseen sopivia neuvoja ja muokattiin niitä sopivaksi omaa koulutusta varten.

4 Tietoturvakoulutuksen toteuttaminen

Tietoturvakoulutus toteutettiin yhdessä yrityksen tietoturvaryhmän kanssa. Tietoturvaryhmä osallistui varsinkin koulutusmateriaalin tuottamiseen ja koulutustilaisuuden suunnitteluun. Tässä opinnäytetyössä työvaiheet käytiin läpi yhdellä toimintatutkimuksen iteraatiolla.

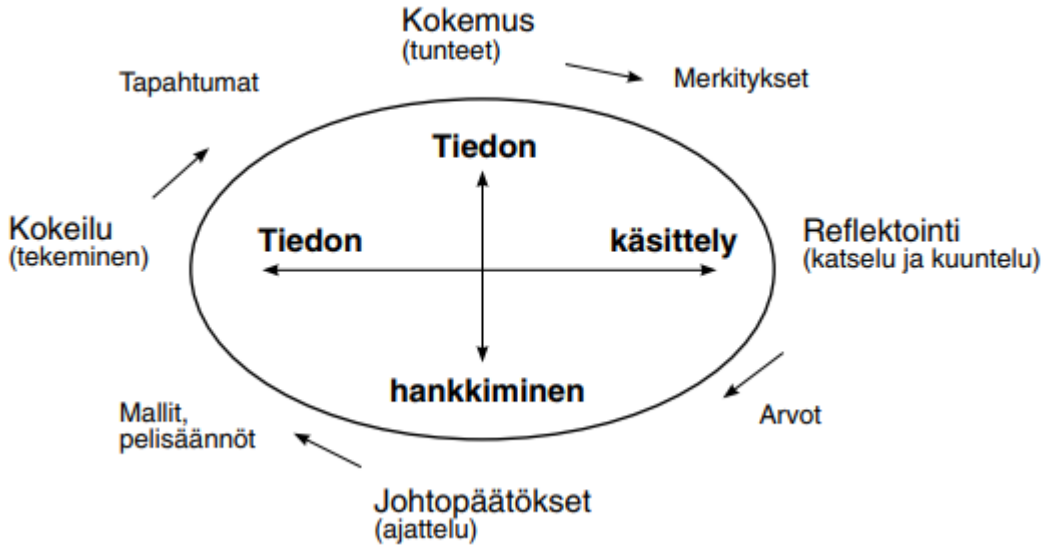
4.1 Kehityskohteen tunnistaminen

Kehityskohteen tunnistamisvaiheessa tavoitteena oli löytää tietoturvaan ja varsinkin uuden tietosuoja-asetuksen vaatimuksiin liittyvä aihe. Yhdessä tietoturvatiimin kanssa mietittiin keskeisiä kehityskohteita, joita olisi mahdollista toteuttaa opinnäytetyönä. Tässä opinnäytetyössä kehittämiskohteeksi nousi yrityksen henkilöstön tietoturvan taso. Yrityksessä pidetyt aikaisemmat tietoturvakoulutukset eivät olleet vielä kattaneet uuden tietosuoja-asetuksen vaatimuksia.

Tietoturvakoulutus nähtiin hyödylliseksi myös osana sitä prosessia, jolla yritys pystyy tarpeen tullessa osoittamaan, että tietosuojauudistukseen ollaan valmistauduttu Henkilöstöön liittyvät tietoturvatekijät ovat mahdollisesti tietojen luottamuksellisuuden, käytettävyyden ja eheyden uhkana. Tämän koulutuksen tarkoituksena oli siis parantaa henkilöstön tietoturvatasoa ja näin vähentää myös mahdollisia tietovuotoja ja muita henkilöstöstä johtuvia mahdollisia tietoturvauhkia (VAHTI 2008).

4.2 Suunnittelu

Tietoturvakoulutuksen suunnittelu tehtiin yhdessä yrityksen tietoturvaryhmän kanssa. Tarkoituksena oli luoda koulutus, joka olisi sisällöltään ymmärrettävissä ilman erillistä kouluttamista. Sen tulisi kuitenkin myös toimia luennon kaltaisessa tilaisuudessa koulutusmateriaalina. Koulutuksen suunnittelussa otettiin huomioon millaisia esimerkkejä tulisi esimerkiksi käyttää, jotta jokainen yrityksen henkilö pystyisi ymmärtämään ne. Tästä syystä koulutukseen lisättiin myös sanasto osio, minkä tarkoituksena oli helpottaa materiaalin ymmärtämistä ilman koulutusta.



Kuva 2: Kolbin kehä

Brainstorming menetelmää käytettiin alkuvaiheessa, kun päätettiin alustavia otsikkoja sisällölle. Brainstorming eli suomeksi aivoriihi on luovan ongelmanratkaisun menetelmä. Siinä on tarkoituksena keksiä ideoita ongelmiin, joihin ei ole yhtä vastausta. Ensimmäisessä kokouksessa tietoturvaryhmän kanssa pidettiin vapaamuotoinen brainstorming sessio, missä mietittiin aiheita mitä koulutuksen tulisi käsitellä. Brainstorming sessioista saatujen tulosten avulla pystyttiin aloittamaan sisällön tuottaminen koulutusta varten.

Koulutuksen suunnittelussa käytettiin apuna Valtiovarain Ministeriön Valtiohallinnon tietoturvallisuuden johtoryhmän eli VAHTI kirjoittamaa tietoturvakouluttajan opasta. Oppaasta löytyy neuvoja siihen, kuinka esimerkiksi ryhmien koot ja aikataulu täytyy ottaa huomioon tietoturvakoulutuksen suunnittelussa. Koulutuksessa tuli myös ottaa huomioon, kuinka saada kuuntelijat heti kiinnostumaan aiheesta (VAHTI 2006).

Ihmiset oppivat helpommin luomalla yhteyden kokemuksiin ja tunteisiin. Jos koulutuksessa sanotaan, että tuntematon ihminen saattaa päästä liikkumaan valvomatta yrityksen tiloissa, ei tämä välttämättä saa oikeaa vaikutusta aikaan. Kun kuuntelijoita varoitetaan siitä, että kyseinen henkilö saattaa päästä käsiksi naulakossa oleviin tavaroihin, saa kuuntelija siitä helpommin mieleen jäävän muistikuvan (VAHTI 2006).

Koulutusmateriaalin suunnittelussa tuli myös vastaan se, että helposti kaikki ohjeistukset menivät siihen malliin, että älä tee sitä tai älä tee tuota. Tämä jättää lukijalle ja kuulijalle enemmän kysymyksiä, kuin suorat ohjeet, joissa kerrotaan mitä tulee tehdä tilanteessa. Kieltomuodot antavat myös helposti negatiivisemman kuvan kuin on tarve.

Tietoturvakoulutusta suunnitellessa piti myös ottaa huomioon ryhmien koko. Valtiovarainministeriön julkaisemassa tietoturvakouluttajan oppaassa sanotaankin, että yli 30 henkilölle pidetyssä koulutuksessa ihmisillä on suurempi kynnys kysyä kysymyksiä kuin pienemmissä ryhmissä. Tämä tuli ottaa huomioon koulutuksessa ja koulutusta pidettäessä kuuntelijoita pyrittiinkin rohkaisemaan kysymään kysymyksiä, mikäli jotain jäi epäselväksi (VAHTI 2006).

4.3 Koulutuksen järjestäminen

Koulutuksen pituudeksi valittiin yksi tunti. Ennen varsinaista koulutusta pidettiin kenraaliharjoitus, johon osallistui tietoturvaryhmän lisäksi yksi työntekijä, joka ei ollut osallistunut koulutusmateriaalin tekemiseen. Harjoituksen tarkoituksena oli varmistaa, että koulutuksen sisältö oli ymmärrettävää ja selkeää.

Harjoituksesta tullut palaute oli pääosin positiivista. Materiaali ja koulutus olivat arvioinnin mukaan helposti ymmärrettävää ja opettavaa. Koulutuksen kesto venyi hieman päälle tunniksi, sillä keskustelua syntyi paljon. Varsinkin omakohtaisia kokemuksia oli paljon ja näitä tulisi suuremmalle yleisölle pidettävässä koulutuksessa välttää, jotta koko materiaali saataisiin käytyä läpi. Harjoituksessa nämä kuitenkin osoittautuivat hyväksi materiaaliksi itse varsinaista koulutusta varten.

Harjoitusta pidettäessä tuli vastaan sanoja, jotka vaativat tarkempaa selitystä. Harjoituksesta saadun palautteen jälkeen kävin vielä esityksen läpi. Tarkoituksena oli saada siitä karsittua pois kuulijalle epäselvät asiat, tai saada niiden selitykset lisättyä suoraan esitykseen. Koulutuksen sisällön täytyi olla hyvin selkeä, koska tunnin pituinen luento ei jätä paljoa varaa epäselvyyksien selvittelyyn.

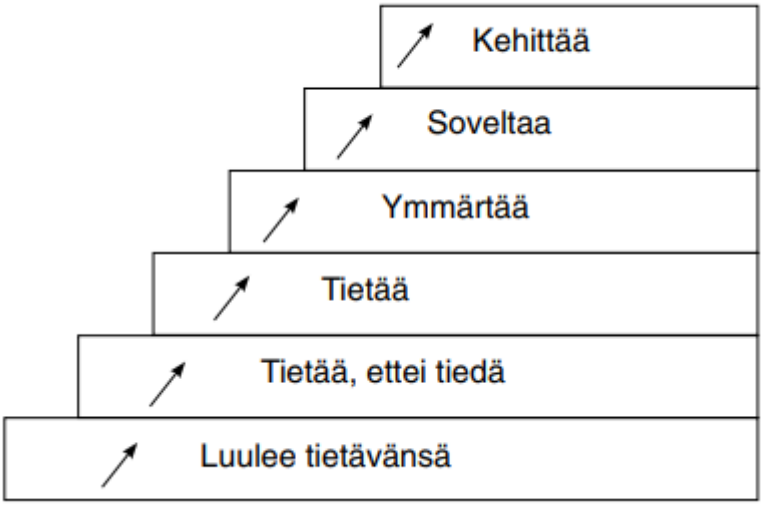
Varsinainen koulutus pidettiin kaksi kertaa, jotta siihen saataisiin mahdollisimman paljon osallistujia. Ensimmäinen koulutus pidettiin aamulla. Siihen osallistui noin kymmenen henkilöä. Koulutus meni hyvin, vaikka sen kesto jäikin hieman lyhyemmäksi kuin mitä siihen oltiin varattu. Tämä johtui siitä, että pienessä ryhmässä keskustelua ei syntynyt paljoa. Kysymykset saatiin myös nopeasti käytyä läpi.

Seuraava koulutus oli päivällä ja tähän osallistui noin kolmekymmentä henkilöä. Tämä koulutus meni myös hyvin, ja se herätti paljon enemmän keskustelua kuin aamun koulutus. Aikaa oli kuitenkin vain yksi tunti, joten keskustelua jouduttiin hieman rajoittamaan.

Molempien koulutusten synnyttämä keskustelu liittyi pääosin tietosuoja-asetuksen tuomiin vaatimuksiin. Suurin osa yrityksen henkilöstöstä oli jo tietoinen uudesta asetuksesta, mutta ei tarkemmin siitä millaisia vaatimuksia tämä toisi heille sekä yritykselle. Koulutuksen tarkoituksena oli myös saada yrityksen henkilöstöä kiinnostumaan itse ottamaan selvää, millaisia uusia oikeuksia tietosuoja-asetus heille toisi. Tämän tarkoituksena oli saada levitettyä tietoturvakulttuuria heidän omasta toimestaan.

4.3.1 Tietoturvakoulutuksen sisältö

Koulutuksen sisältö selvitettiin yhdessä yrityksen tietoturvatiimin kanssa. Materiaalin kirjoitusprosessi alkoi selvittämällä mitkä osa-alueet koulutuksen täytyisi kattaa. Päädyttiin siihen, että tietoturvakoulutus sisältäisi kaikki henkilöstöä koskevat ohjeistukset liittyen tietoturvaan. Aihealueet valittiin tutkimalla julkisia tietoturvaohjeistuksia, tietosuoja-asetuksen vaatimuksia ja ottamalla huomioon yrityksen vaatima yksilöinti.



Kuva 3: Oppimisen portaat (Sydänmaanlakka 2000)

Yrityksen tietoturvasivuilla olevassa PowerPoint diaesityksessä toistuu myös samat asiat useaan kertaan eri dioissa. Nämä toistuvuudet päätettiin sisältää eri dioihin siltä varalta, että työntekijä katsoo vain yhden kohdan materiaalista, esimerkiksi etätyöskentelyn. Jos toistoa ei olisi, saattaisi materiaalia lukevalta henkilöltä jäädä tärkeitä osia pois koulutusta kerratessa. Tämä toi selkeyttä itsenäistä opiskelua varten. Koulutusta varten olisi kuitenkin voinut jälkeenpäin ajatellen tehdä toisen version, mistä toisto olisi poistettu.

4.3.2 Työpaikalla työskentely

Työasioiden jakaminen kuuluu jokaisen työpaikan toimintaan. Käsitellessä luottamuksellisia tietoja ja varsinkin henkilötietoja tulee kuitenkin ottaa huomioon, ettei jokainen työasia kosketa kaikkia yrityksen työntekijöitä. Tietosuoja-asetuksen yksi pääasioita onkin se, että henkilötietojen käsittelyyn täytyy aina olla peruste, kuten palvelupyyntö asiakkaalta. Tämä voi olla esimerkiksi asiakaspalvelun toteuttama asiakkaan pyyntö saada selville kuinka paljon heidän tilillään on saldoa. Henkilötietoja tulee kuitenkin käsitellä vain työperusteisesti, eikä työntekijöiden suorittamaan tietojen käsittelyyn saa osallistua ilman siihen perusteltavaa tarvetta (Tietosuoja.fi 2018).

Myös työpaikalla on oleellista, että arkaluontoiset tiedot eivät ole näkyvillä henkilöille, joille ne eivät kuulu. Tämän takia on tärkeää, että esimerkiksi paperit jotka sisältävät näitä tietoja, kuten henkilötietoja, tulee säilyttää tavalla jolla ne eivät ole ulkopuolisille näkyvillä. Yrityksen tiloissa kuitenkin liikkuu esimerkiksi siivoojia, joille nämä tiedot eivät kuulu (Itäsuomen yliopisto 2017).

Kulunvalvonta on tärkeä osa fyysistä tietoturvaa. Jokaisen yrityksen työntekijä voi osallistua kulunvalvontaan, ja huomioida tiloissa liikkuvat ulkopuoliset. Tiloihin kutsutuista vieraista tulee huolehtia ja varmistaa etteivät he liiku tiloissa ilman valvontaa. Näin voidaan varmistaa se, ettei esimerkiksi naulakosta päästä varastamaan henkilöstön tavaroita, kuten puhelimia tai kannettavia tietokoneita (VAHTI 2006).

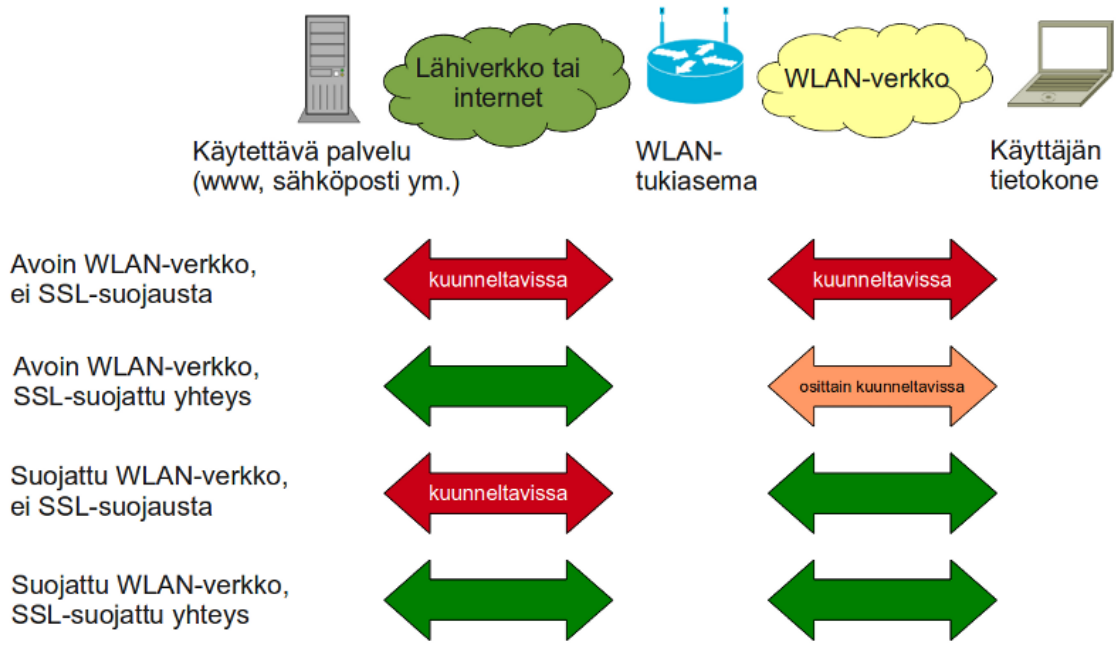
Vieraiden henkilöiden tunnistaminen työtiloissa on tärkeää myös yrityksen salaisten asioiden suojaamisen kannalta. Luottamuksellisista asioista tulisikin keskustella vain silloin, kun on varmuus, ettei tiloissa ole henkilöitä joille nämä asiat eivät kuulu. Tietokoneet tulisi myös lukita aina kun niiden luota poistutaan. Näin voidaan välttää tietovuotoja, sekä mahdollisten haittaohjelmien asentamista yrityksen tietokoneille (VAHTI 2006).

4.3.3 Etätyöskentely

Työn tekoon käytettäviä päätelaitteita tulisi käyttää pelkästään itse työntekijä. Laitteille on usein tallennettu esimerkiksi salasanoja järjestelmiin ja tiedostoja joissa on arkaluontoisia tietoja. Päätelaitteet tuleekin olla aina lukittuna, kun niitä ei olla valvomassa tai käyttämässä (Itäsuomen Yliopisto 2017).

Etätyöskentelyyn tulee käyttää vain siihen tarkoitettuja laitteita. Nettikahviloiden, hotellien tai kirjastojen tietokoneissa voi olla esimerkiksi asennettuna haittaohjelmia. Nämä haittaohjelmat voivat saada haltuun kirjautumistietosi (VAHTI 2006).

VPN-yhteyttä tulisi käyttää erityisesti, kun töitä täytyy tehdä vieraissa tai avoimissa verkoissa. VPN tarkoittaa virtuaalista erillisverkkoa. Se on tapa, jolla voidaan luoda turvallinen yhteys yrityksen verkkoon, luomalla näennäisesti yksityinen verkko.



Kuva 4: Langattomat verkot (Viestintävirasto.fi)

Vieraaksi verkoksi luetaan esimerkiksi junan verkko. On mahdollista, että joku henkilö on virittänyt oman verkkonsa ja nimennyt sen samalla tavalla kuin junan verkon. Tämän takia VPN-yhteyttä täytyy aina käyttää, kun ei voida olla täysin varmoja verkon turvallisuudesta. Näin voidaan välttää mies välissä hyökkäyksiä, jossa viestintäreittiin tunkeutuu viestijöiden huomaamatta kolmas osapuoli. Omassa kotiverkossakin olisi hyvä käyttää VPN-yhteyttä, mutta se ei ole niin tärkeää kuin julkisissa verkoissa sen käyttäminen (Viestintävirasto 2011).

Etätyöskennellessä kuten myös työpaikalla työskennellessä henkilötietoja ja muita arkaluontoisia papereita sisältävät paperit tulee säilyttää niin, ettei tiedot paljastu sivullisille. Kotona olevia papereita ja tietovälineitä tulisi myös säilyttää paikassa, missä ne eivät ole suoraan näkyvillä. Myös kotona säilytettävien papereiden ja muiden tietovälineiden hävittäminen täytyy tehdä tietoturvallisella tavalla, kuten silppuamalla. Tietovuoto voi sattua esimerkiksi sopimusten tai henkilötietoja sisältävien papereiden löydyttyä paperinkeräyksestä tai roskalaatikosta (VAHTI 2006).

4.3.4 Julkisella paikalla työskentely

Julkisella paikalla työskentelyyn pätee etätyöskentelyn säännöt, jonka lisäksi täytyy myös olla erityisen varovainen, ettei ulkopuoliset näe tai kuule heille kuulumattomia asioita. Julkisella paikalla töitä tehdessä täytyykin käyttää näytönsuojaa, jolla estetään vierestä katselu.

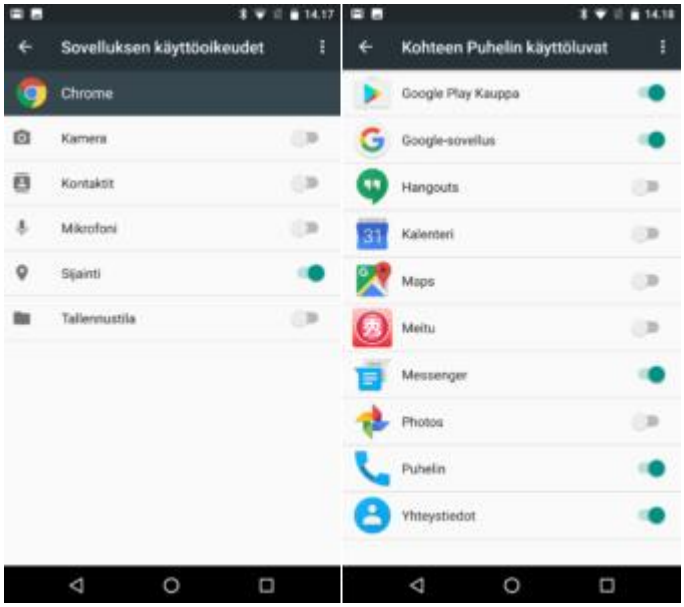
Luottamuksellisista asioista keskustelua tulisi välttää julkisilla paikoilla. Jos luottamuksellisia tietoja täytyy jakaa esimerkiksi kahvilassa, tulisi asiakkaista puhuessa käyttää lyhenteitä, tai muita tapoja joilla osapuolia ei voida tunnistaa keskustelusta. On tapauksia missä asiakkaita on menetetty, kun heidän asioistaan on keskusteltu julkisilla paikoilla. Suomi on pieni maa, eikä koskaan voi olla varma kuka on kuulemassa.

Erityistä huolellisuutta tulee myös noudattaa, kun kuljetetaan henkilötietoja tai muita arkaluonteisia tietoja salaamattomassa muodossa kuten paperilla tai muistitikulla. Täytyykin olla varovainen, ettei näitä jää esimerkiksi junan penkeille (VAHTI 2006).

4.3.5 Mobiililaitteet

Mobiililaitteille on usein tallennettu salasanoja yrityksen järjestelmiin. Nämä tulisi suojata turvatoimilla, kuten suojakoodilla jota vaaditaan aina kun laite avataan lukituksesta. Sormenjälki- tai kasvontunnistus ovat myös turvallisia, mutta kuvion piirtoa ei tulisi käyttää sen heikon tietoturvan takia. Kuvion piirron voi saada helposti selville katsomalla vierestä, tai siitä ruutuun jääneistä tahroista.

Mobiililaitteiden tietoturvapäivitykset tulee asentaa viipymättä niiden tullessa tarjolle. Ennen sovellusten asentamista mobiililaitteille, tulee varmistua niiden turvallisuudesta. Täytyy myös harkita mitä oikeuksia antaa ohjelmille. Esimerkiksi vakoileva sovellus saattaa pyytää sinua antamaan oikeudet lukemaan ja lähettämään tekstiviestejä tai sähköposteja ilman varsinaista oikeaa syytä (Viestintävirasto 2017).



Kuva 5: Esimerkki sovellusten vaatimista oikeuksista Android puhelimella

Laitteita ei myöskään saisi jättää paikkoihin, mistä niitä on helppo varastaa kuten auton penkille näkyville. Kaikki työhön käytettävät päätelaitteet tulisikin pitää valvotussa tilassa, tai mukana vaikka niitä ei juuri sillä hetkellä käytettäisi. Näytölle tulleiden ilmoitusten näkymistä tulisi säätää niin, ettei ruudulle tule näkyville luottamuksellista tietoa, jos puhelin tai tabletti on esimerkiksi jäänyt pöydälle

4.3.6 Salasanat ja vahva tunnistautuminen

Salasanoihin liittyvät turvatoimet ovat yleisesti samat kaikkialla. Salasanojen tulee olla vahvoja. Salasanojen vahvuudessa tärkeintä on se, että ne ovat pitkiä sekä uniikkeja. Salasanat ei saisi esimerkiksi olla suoraan sanakirjasta löytyviä sanoja, tai yleisesti käytettyjä salasanoja. Vahvoilla salasanoilla voidaan välttää varsinkin brute force hyökkäyksiä, joissa hyökkääjä yrittää selvittää käyttäjän salasanan kokeilemalla kaikkia mahdollisia kirjain, numero ja merkki yhdistelmiä. Salasanojen tulisi olla uniikkeja sen takia, että hyökkääjät käyttävät usein vuotaneita salasanalistoja, joiden avulla he voivat kokeilla erilaisia yleisiä käytettyjä salasanoja (VAHTI 2006).

Salasanaholvin käyttöä suositellaan. Salasanaholvi on sovellus, joka tallentaa järjestelmien salasanat yhteen paikkaan. Näin yhden salasanan takana voi olla satoja eri järjestelmien salasanoja ja henkilön täytyy huolehtia vain yhden salasanan muistamisesta.

Samaa salasanaa ei tulisi käyttää useaan kertaan, koska jos samaa salasanaa käytetään useassa palvelussa, sen selvitessä saadaan helposti haltuun tämän käyttäjän muidenkin palveluiden käyttäjätilit. Salasana tulisi myös vaihtaa vain, jos epäillään jonkun saaneen sen selville. Näin vähennetään tapauksia, joissa salasana unohtuu sekä useiden eri salasanoja sisältävien muistilappujen määrä (VAHTI 2006).

Salasanojen kirjoittaminen ylös on kuitenkin sallittua, mutta näin tehdessä täytyy huomioida mihin salasana kirjoitetaan ja kuinka sitä säilytetään. Esimerkiksi tietokoneen viereen jätetty salasanavihko ei ole turvallinen. Käytettäessä muistikirjaa tulisi se säilyttää niin, ettei siinä säilytettäviä salasanoja voida selvästi yhdistää siihen järjestelmään missä salasanaa käytetään. Salasanat voidaan myös kirjoittaa talteen niin, että niistä jätetään esimerkiksi osa pois. Jos palveluissa on mahdollisuus käyttää lisätunnistusmenetelmiä, kuten salasanan lisäksi koodia tekstiviestillä tai koodisovellusta, suositellaan näitä käyttämään.

4.3.7 Luottamuksellisen tiedon käsittely

Päätelatteilla eli kaikilla laitteilla joilla käsitellään tietoja ei saa säilyttää luottamuksellisia tai arkaluontoisia tietoja sen jälkeen, kun niitä ei enää tarvita. Uuden tietosuoja-asetuksen yksi velvoite on pitää henkilötietojen käsittely pienimmässä mahdollisessa määrässä. Henkilötietoihin ei siis saa koskea, ellei siihen ole perusteltavaa syytä (Tietosuoja.fi 2018).

Mitä useammassa paikassa henkilötietoja on tallennettuna, sitä vaikeampaa niitä on tarpeen tullessa poistaa tai antaa niiden sijainnista tieto asiakkaalle tämän vaatiessa. Uusi tietosuoja-asetus vaatii sen, että kaikki asiakkaan henkilötiedot voidaan poistaa kaikista yrityksen järjestelmistä tämän sitä vaatiessa, jos niiden säilyttämiseen ei ole lain velvoittamaa syytä. Asiakas voi myös pyytää listauksen siitä, mitä kaikkea tietoa yrityksellä hänestä löytyy ja missä järjestelmissä nämä tiedot ovat (Tietosuoja.fi 2018).

Kaikki luottamuksellisia tietoja sisältävät paperit, muistitikut ja ulkoiset kovalevyt tulee hävittää turvallisesti. Niitä ei saa heittää esimerkiksi suoraan roskikseen tai paperinkeräykseen. Luottamuksellista aineistoa tuottaessa täytyy ne merkitä niin, ettei kukaan pääse katsomaan niitä vahingossa tietämättä niiden olevan luottamuksellista aineistoa. Luottamuksellista tietoa jakaessa täytyy ensin varmistua vastapuolen henkilöllisyydestä, ja siitä että tarvittavat turvatoimet on otettu huomioon (VAHTI 2006).

Tietoa synkronoidessa täytyy miettiä mitä synkronoidaan ja minne. Esimerkiksi asiakkaiden henkilötietoja tai muita luottamuksellisia tietoja ei saa synkronoida henkilökohtaisiin pilvipalveluihin, kuten Dropbox, Google Drive tai iCloud Drive. Yrityksen omaan IT-ympäristöön näitä saa tallentaa, mutta täytyy ottaa huomioon mikä on oikea paikka henkilötiedoille ja niiden tallentaminen täytyy pitää pienimmässä mahdollisessa määrässä.

4.3.8 Turvallinen käyttö

Turvallinen käyttö osio kattaa ohjeistuksia siitä, kuinka suojautua henkilöstöön kohdistetuilta hyökkäyksiltä. Yrityksen työntekijöille voi tulla esimerkiksi soittoja, joilla yritetään kalastella omia, yrityksen tai asiakkaiden tietoja. Keskustellessa näistä kuten muista luottamuksellisista tiedoista, tulee aina varmistua vastapuolen henkilöllisyydestä. Nykyään vaaditaan kaksiosainen tunnistautuminen, eli pelkkä henkilötunnus ei esimerkiksi enää riitä.

Täytyy myös varmistaa, että on oikealla verkkosivulla, sillä internetistä löytyy useita huijaussivuja. Esimerkiksi www.srnartum.fi voi nopeasti luettuna näyttää samalta kuin www.smartum.fi. Useasti huijaussivujen web-osoite on aivan erilainen kuin sivun mitä se yrittää kopioida, mutta se näyttää muuten samalta. Näillä yritetään kalastella kirjautumistietoja, kuten esimerkiksi pankkitietoja tai yrityksen järjestelmien salasanoja (Itäsuomen Yliopisto 2017).

Ennen tuntemattoman lähettäjän sähköpostiviestissä olevien lähteiden avaamista täytyy varmistaa, että niiden sisältö on turvallista, sillä näissä voi olla haittaohjelmia. Myös tutulta lähettäjältä tulleiden liitteiden avaamista tulee harkita, jos niissä näkyy poikkeavaisuuksia. Tämä on voinut saada haittaohjelman, joka leviää sähköpostilla (Itäsuomen Yliopisto 2017).

4.3.9 Poikkeamat

Poikkeamien havaitseminen on oleellinen osa tietoturvallisuutta. Poikkeamia voi olla esimerkiksi tuntematon esine tai henkilö työpaikalla. Myös kohdistetut huijaussähköpostit sekä soitot tai päätelaitteen erikoinen toiminta voidaan lukea poikkeamiksi. Erilaisia poikkeamia varten täytyy olla valmiit suunnitelmat.

Päätelaitteen tai muun henkilötietoja sisältävän paperin tai ulkoisen kovalevyn kadotessa täytyy tehdä ilmoitus tietosuojavaltuutetulle, mikäli voidaan olettaa, että siitä aiheutuu tietovuoto. Ilmoitus täytyy tehdä 72 tunnin sisällä tietovuodon tapahtumisesta. Jos päätelaitteet on suojattu oikein, eikä ole mitään syytä olettaa, että tietoihin päästään käsiksi, ei ilmoitusta tarvitse tehdä. Tämän takia on tärkeää, että kaikki turvatoimet päätelaitteen suojaamiseksi ovat ajan tasalla. Näin voidaan välttää tietovuotojen syntymistä.

4.4 Arviointi

Arvioinnin tarkoituksena on löytää parannettavaa liittyen kehityskohteeseen. Tietoturvakoulutuksen vaatiessa päivitystä on hyvä palata siihen, millaista palautetta aikaisemmasta koulutuksesta on annettu. Arvioinnin perusteella voidaan löytää kehityskohteita aikaisemmasta koulutuksesta ja näin parantaa sitä.

Tietoturvakoulutus sai hyvää palautetta. Koulutus oli palautteen mukaan kuulijan kannalta hyvin selkeä ja se eteni loogisesti. Esitys aiheutti aitoa keskustelua ja mielenkiintoa. Vaikka koulutusmateriaali oli selkeää, sai se paljon keskustelua aikaan. Tunnin pituinen tietoturvakoulutus ei kuitenkaan antanut tarpeeksi aikaa kaikille kysymyksille. Tulevaisuudessa pidettäville koulutuksille olisi hyvä antaa enemmän aikaa ja esimerkiksi pitää vähintään kaksi tunnin pituista luentotyyppistä koulutusta. Näin kysymysten vastaamiseen ja materiaalin selventämiseen jäisi tarpeeksi aikaa, eikä keskustelua tarvitsisi keskeyttää aikamääreiden takia.

4.5 Tulosten esittely

Viimeinen vaihe tämän kaltaisessa toimintatutkimuksessa on siinä aikaan saatujen tulosten esittely, eli tässä tapauksessa opinnäytetyön kirjoittaminen. Opinnäytetyötä kirjoittaessa täytyi ottaa huomioon yrityssalaisuuksien säilyttäminen, sekä se ettei siitä paljastu mahdollisia tietoturvaheikkouksia. Myös lupa kaikkeen opinnäytetyössä julkaistuun tietoon, kuten yrityksen kanssa yhteystyössä tehtyyn koulutusmateriaaliin täytyi pyytää.

Koulutusmateriaalin liittäminen opinnäytetyöhön vaati myös tiettyjä toimenpiteitä, ennen kuin siitä voitiin tehdä julkista. Muutama dia itse PowerPoint esityksestä poistettiin sen takia, että niissä ollut tieto oli täysin yksilöityä eikä siitä ollut hyötyä itse opinnäytetyötä varten. Myös kaikki henkilötiedot, sekä tiedot liittyen yrityksen järjestelmiin ja muihin yksilöiviin tekijöihin on riisuttu pois liitteenä olevasta materiaalista.

5 Yhteenveto ja pohdintaa

Opinnäyteyön aloitusvaiheessa oli vielä epäselvää minkälainen lopputuloksesta tulisi. Työ alkoi työnantajan kanssa keskustelemalla mahdollisista opinnäytetyöaiheista. Aihe rajoittui tietosuoja-asetuksen tuomiin uusiin vaatimuksiin. Opinnäytetyön piti aluksi olla yleispätevä ohjeistus henkilötietojen käsittelijöille. Aiheen selkeytyessä tein tutkimussuunnitelman, joka kattoi opinnäytetyön aikataulun, työvaiheet sekä alustavan sisällön.

Työn alkuvaiheessa kuitenkin huomattiin, ettei ensimmäinen suunnitelma opinnäytetyöstä ollut tarpeeksi selkeä. Alkuperäinen suunnitelma tehdä henkilötietojen käsittelyä varten ohjeet osoittautui hankalaksi sen takia, että oli vaikeaa rajata kenelle ohjeet pitäisi tehdä ja minkä osan henkilöstöstä nämä tulisi lukea. Tietoturvaryhmän kanssa päädyttiinkin siihen, että koulutuksesta tulisi yleispätevä tietoturvakoulutus koko yrityksen henkilöstölle. Sen tuli myös kattaa tietosuoja-asetuksen tuomat vaatimukset liittyen henkilötietojen käsittelyyn, mutta ei rajoittaa koulutusta pelkästään käsittelemään tietosuojaa, vaan myös yleisiä tietoturvaohjeita.

Tietosuoja-asetus velvoittaa jokaisen henkilötietoja käsittelevän yrityksen pystyvän osoittamaan, että heidän henkilötietojen käsittely on tarpeeksi turvallisella tasolla. Tietoturva yleisesti ja varsinkin henkilöstön koulutus on tärkeä osa prosessia, jolla voidaan näyttää, että tietosuoja-asetuksen vaatimukset on otettu huomioon yrityksen toiminnassa.

Tietoturvakoulutuksen tekeminen ja varsinkin sen pitäminen oli opettava kokemus. Sen suunnittelussa tuli vastaan useita erilaisia haasteita, joita pääsin ratkaisemaan yhdessä yrityksen tietoturvaryhmän kanssa. Koulutuksen jättämästä vaikutuksesta olisi voinut saada konkreettisemman kuvan, jos tätä varten olisi esimerkiksi tehty jonkinlaisia tehtäviä tai lomake, mihin koulutukseen osallistuneet olisivat voineet vastata koulutuksen jälkeen.

Lähteet

Sähköiset

Baskerville, R. 1999. Investigating Information Systems with Action Research. Viitattu 1.4.2018 http://aisel.aisnet.org/cgi/viewcontent.cgi?article=2518&context=cais

Ekatuo, T. 2014. Ulla Suojanen: Toimintatutkimus ammatillisen kehittymisen välineenä https://metodix.fi/2014/05/19/suojanen-toimintatutkimus/ Viitattu 7.4.2018

Itäsuomen Yliopisto. 9/2017. Henkilöstön Tietoturvaopas. Viitattu 3.3.2018. https://www.uef.fi/documents/11039/196003/henkiloston-tietoturvaopas.pdf/d3ddaff4-c88d-4be9-ba06-8cf845f57bc3

Metivier, B. 4/2017. Fundamental Objectives of Information Security: The CIA Triad. Viitattu 13.5.2017 https://www.sagedatasecurity.com/blog/fundamental-objectives-of-information-security-the-cia-triad

OpiTietosuojaa.fi 12/2016. Yleistä Tietosuojasta. Viitattu 12.5.2017 https://opitietosuojaa.fi/index.php/fi/aloitus/tietosuoja

Tietosuoja.fi 9/2013. Tietosuoja-aiheista sanastoa. Viitattu 12.5.2018 http://www.tietosuoja.fi/fi/index/sanasto.html

Tietosuoja.fi. 3/2018. EU:n tietosuojauudistus. Viitattu 25.3.2018. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html

VAHTI 11/2006 Tietoturvakouluttajan opas. Viitattu 15.3.2018 https://www.vahtiohje.fi/web/guest/11/2006-tietoturvakouluttajan-opas

VAHTI 10/2006. Henkilöstön Tietoturvaohje. Viitattu 3.3.2018 https://www.vahtiohje.fi/c/document_library/get_file?uuid=c338d07d-ac04-4884-b941-1554d07ae41f&groupId=10128

VAHTI 2/2008. Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta. Viitattu 4.3.2018 https://www.vahtiohje.fi/web/guest/2/2008-tarkein-tekija-on-ihminen-henkilostoturvallisuus-osana-tietoturvallisuutta

VAHTI 8/2009. Hallinnollinen turvallisuus. Viitattu 16.5.2018 https://www.vahtiohje.fi/web/guest/hallinnollinen-turvallisuus

Viestintävirasto. 2011. Ohje 2/2011 Langattomien verkkojen tietoturvasta. Viitattu 4.4.2018. https://www.viestintavirasto.fi/ohjausjavalvonta/ohjeetjajulkaisut/ohjeidentulkintojensuositustenjaselvitystenasiakirjat/ohje22011langattomienverkkojentietoturvasta.html

Viestintävirasto. 10/2017. Matkapuhelimen turvallinen käyttö. Viitattu 3.3.2018 https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvaohjeet/laitteenturvallinenkaytto/matkapuhelin.html

Kuvat

Liitteet

Liite 1: Agenda ja taustaa

Agenda ja taustaa

- EU GDPR, tietosuoja-asetus
  - Voimaan 24.5.2016, siirtymäaika päättyy 25.5.2018 (sanktiot voimaan, korkeimmillaan 20 miljoonaa euroa tai 4% yrityksen vuotuisesta kokonaisliikevaihdosta)
  - Luo uusia velvoitteita henkilötietojen käsittelyä kohtaan
  - Uuden tietosuoja-asetuksen myötä täytyy pystyä osoittamaan, että yrityksen tietoturva on riittävällä tasolla
- Tietoturvan parantaminen yleisesti

- Risto Hämäläinen, Tietojenkäsittelyn opiskelija, opinnäytetyö

smartum

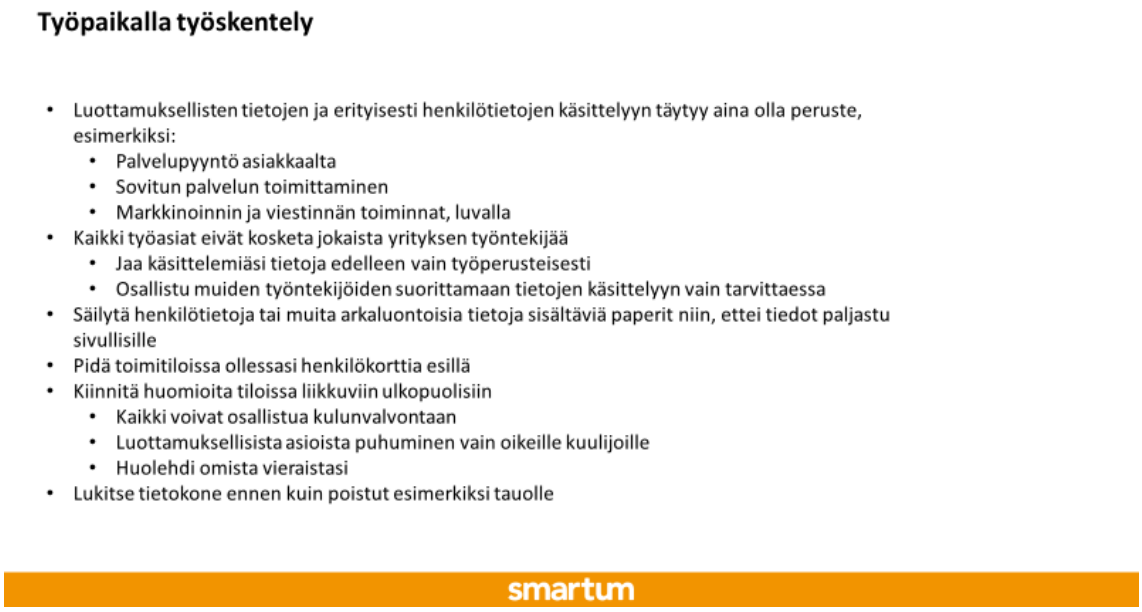
Liite 2: Sanastoa

Sanastoa

- Päätelaite
  - Päätelaitteella tarkoitetaan puhelimia, tabletteja ja kaikkia tietokoneita
- Henkilötieto
  - Henkilötietoja ovat kaikki luonnollista henkilöä tai hänen perhettään/yhteydessä taloudessa elävää koskevat tiedot, esimerkiksi: nimi, henkilötunnus, sijaintitiedot, sähköposti tai tietokoneen IP-osoite
- Tietojen kalastelu
  - Rikollista toimintaa jolla yritetään huijausviestein tai puheluin saada selville luottamuksellisia tietoja, kuten henkilötietoja, salasanoja, pankkitunnuksia tai tilitietoja yms.
- GDPR
  - General Data Protection Regulation, tietosuoja-asetus
- VPN
  - VPN (Virtual Private Network) on tapa, yrityksen verkkoja voidaan yhdistää julkisen verkon yli muodostaen näennäisesti yksityisen verkon. Sillä tarkoitetaan myös yksittäisten etätyöasemien liittämistä yrityksen verkkoon.
- Turvaposti
  - Turvaposti on turvallisempi versio sähköpostista
- Tietovuoto
  - Tietovuodolla tarkoitetaan salaisen tiedon leviämistä

smartum

Liite 3: Työpaikalla työskentely

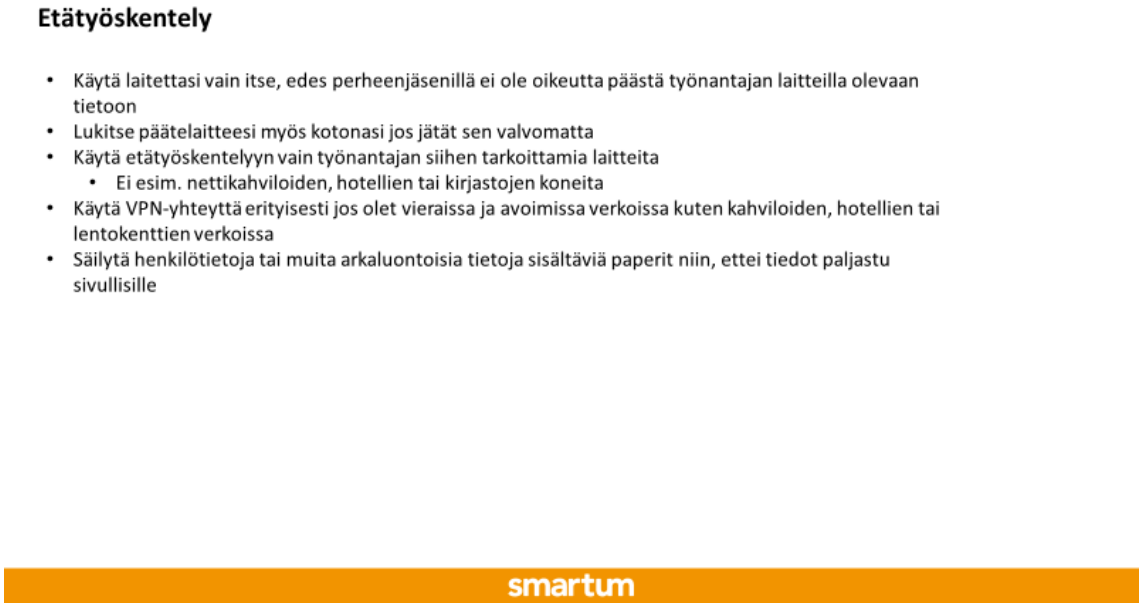


Työpaikalla työskentely

- Luottamuksellisten tietojen ja erityisesti henkilötietojen käsittelyyn täytyy aina olla peruste, esimerkiksi:
  - Palvelupyyntö asiakkaalta
  - Sovitun palvelun toimittaminen
  - Markkinoinnin ja viestinnän toiminnat, luvalla
- Kaikki työasiat eivät kosketa jokaista yrityksen työntekijää
  - Jaa käsittelemiäsi tietoja edelleen vain työperusteisesti
  - Osallistu muiden työntekijöiden suorittamaan tietojen käsittelyyn vain tarvittaessa
- Säilytä henkilötietoja tai muita arkaluontoisia tietoja sisältäviä paperit niin, ettei tiedot paljastu sivullisille
- Pidä toimitiloissa ollessasi henkilökorttia esillä
- Kiinnitä huomioita tiloissa liikkuviin ulkopuolisiin
  - Kaikki voivat osallistua kulunvalvontaan
  - Luottamuksellisista asioista puhuminen vain oikeille kuulijoille
  - Huolehdi omista vieraistasi
- Lukitse tietokone ennen kuin poistut esimerkiksi tauolle

smartum

Liite 4: Etätyöskentely



Etätyöskentely

- Käytä laitettasi vain itse, edes perheenjäsenillä ei ole oikeutta päästä työnantajan laitteilla olevaan tietoon
- Lukitse päätelaitteesi myös kotonasi jos jätät sen valvomatta
- Käytä etätyöskentelyyn vain työnantajan siihen tarkoittamia laitteita
  - Ei esim. nettikahviloiden, hotellien tai kirjastojen koneita
- Käytä VPN-yhteyttä erityisesti jos olet vieraissa ja avoimissa verkoissa kuten kahviloiden, hotellien tai lentokenttien verkoissa
- Säilytä henkilötietoja tai muita arkaluontoisia tietoja sisältäviä paperit niin, ettei tiedot paljastu sivullisille

smartum

Liite 5: Julkisella paikalla työskentely

Julkisilla paikoilla työskentely

Julkisilla paikoilla työskentelyyn pätee etätyöskentelyn säännöt, jonka lisäksi:

- Ole erityisen varovainen, ettei ulkopuoliset näe tai kuule heille kuulumattomia asioita
- Julkisilla paikoilla kannettavalla tietokoneella töitä tehdessä on oltava näytönsuoja joka estää näkymisen vierestä katselemalla
- Vältä luottamuksellisista asioista keskustelua julkisilla paikoilla
- Julkisella paikalla asiakkaista puhuessa käytä asiakkaista lyhenteitä
- Ole erityisen huolellinen jos kuljetat henkilötietoja salaamattomassa muodossa kuten paperilla tai muistitikuilla
- Kuten etätyöskentelyssä, käytä VPN-yhteyttä vieraissa verkoissa

smartum

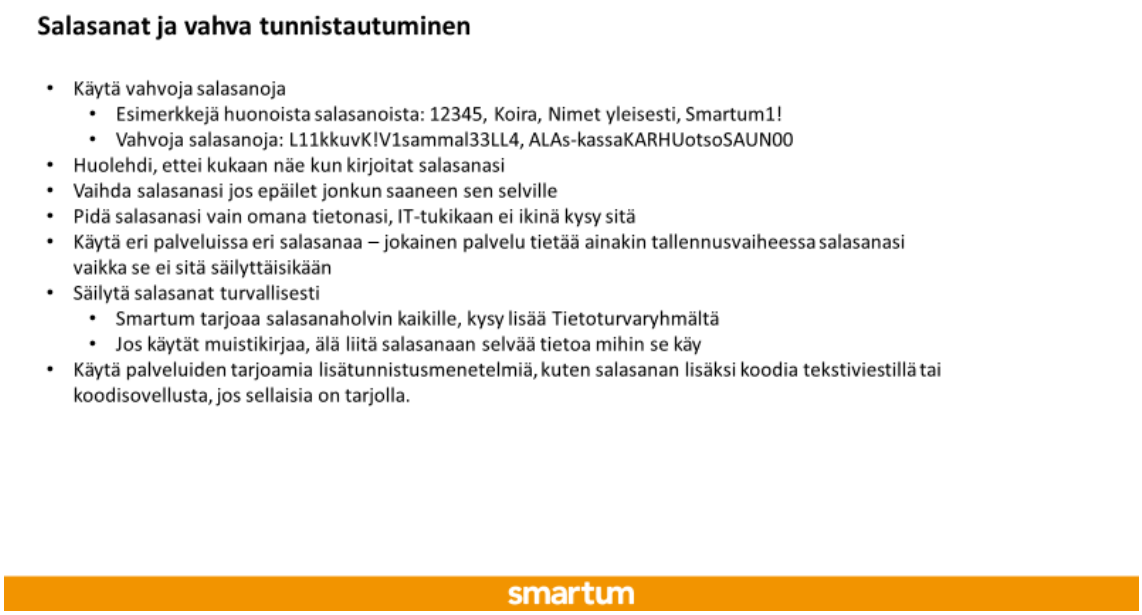
Liite 6: Mobiililaitteet

Mobiililaitteet

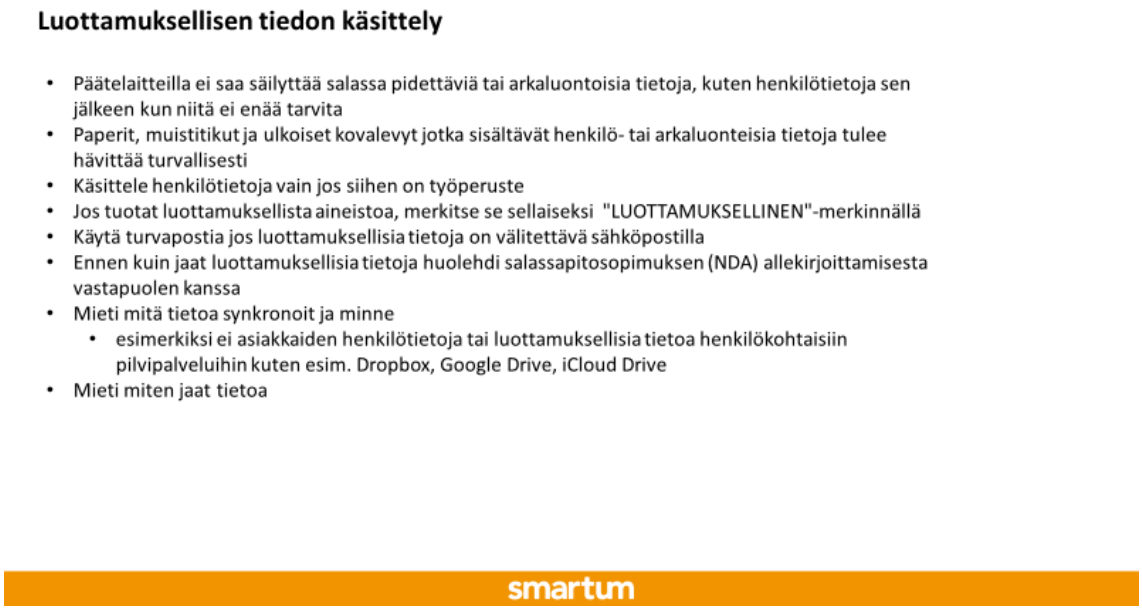
- Suojaa älypuhelimet ja tabletit suojakoodilla, jota kysytään aina kun se avataan lukituksesta
  - Sormenjälki- tai kasvotunnistuskin käy
  - Kuvion piirto on heikko turvaltaan, helppo sivullisen nähdä tai ruudun tahroista
- Käytä vaikeasti arvattavaa suojakoodia (ei esim. 0000, 1234, 2580)
- Käytä myös PIN-koodia, suojaa puhelinliittymän
- Pidä automaattilukitus päällä
- Säädä näytölle tulleiden ilmoitusten näkyvyyttä puhelimen mahdollisesti tarjoamilla tavoilla siten, että luottamuksellista tietoa ei näy lukitulla ruudulla
- Asenna mobiililaitteen tietoturvapäivitykset viipymättä niiden tultua tarjolle
- Harkitse, mitä sovelluksia asennat mobiililaitteelle. Viihdekäyttö on ok, mutta haittaohjelmat leviävät erityisesti "hömppäsovellusten" asentamisen myötä
- Mobiililaitteissa harkitse mitä oikeuksia annat ohjelmille – esimerkiksi vakoileva sovellus voisi pyytää pääsyä lukemaan ja lähettämään tekstiviestejäsi tai sähköpostejasi ilman varsinaista oikeaa syytä
- Älä jätä laitteita valvomatta näkyville, kuten autoon

smartum

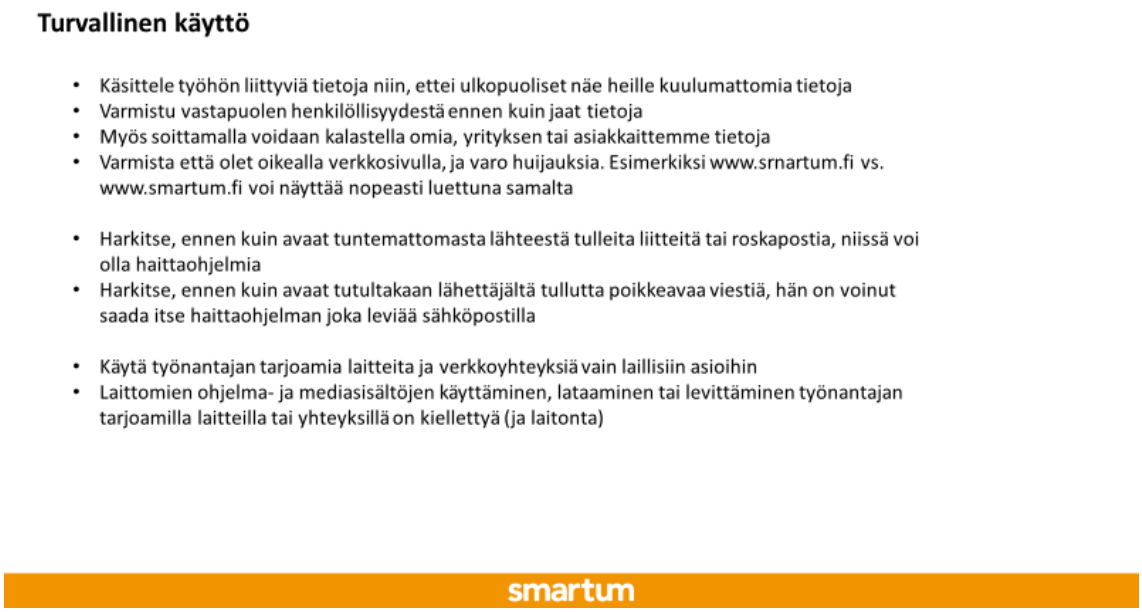
Liite 7: Salasanat ja vahva tunnistautuminen



Liite 8: Luottamuksellisen tiedon käsittely



Liite 9: Turvallinen käyttö



Liite 10: Poikkeamista ilmoittaminen