DIGI- JA VÄESTÖTIETO-VIRASTO

TTTT-malli digiturvalliseen työskentelyyn

VAHTI-hyvät käytännöt tukimateriaali

19.5.2021

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**

Dokumentinhallinta

Omistaja	Kimmo Rousku, Digi- ja väestötietovirasto
Laatinut	Juha Kirves, Kimmo Rousku
Tarkastanut	VAHTI sihteeristö
Hyväksynyt	VAHTI sihteeristö

Version hallinta

versionro	mitä tehty	pvm/henkilö
0.42	Ensimmäinen aihio	18.11.2021 KR, JK
0.75	Ensimmäinen luonnosversio	15.1.2021 KR, JK
0.90	Luonnosversio kommenteille	3.5.2021 KR, JK
1.00	Julkaisuversio	19.5.2021 KR, JK

Sisällysluettelo

TTTT-malli digiturvalliseen työskentelyyn

1 Johdanto

Tämä tukimateriaali on laadittu julkisen hallinnon organisaatioille turvallisen työskentelyn mahdollistamiseksi käsiteltävien tietojen, käytettävien työskentelytilojen ja hyödynnettävien työkalujen näkökulmista. Tukimateriaali pohjautuu julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) asiantuntijoiden kokoamiin riskienhallinnan, toiminnan jatkuvuuden, tietoturvallisuuden ja tietosuojan hyviin käytäntöihin. Hyvien käytäntöjen mukaisesti toimimalla edistämme samalla kyberturvallisuuden toteutumista. Olemme julkaisseet osana Digiturvallinen elämä koulutuksia noin kuuden minuutin TTTT-mallia esittelevän koulutusvideon vapaasti katseltavaksi:

TTTT-malli - video

Edellinen video julkaistiin osana Digiturvallisuus kuntien luottamushenkilöille-verkkokoulutusta. Nimestään huolimatta koulutus sisältää hyviä käytäntöjä meille kaikille

- koulutuksen etusivu

Samoin tulemme julkaisemaan muita lyhyempiä tätä tukimateriaalia edistäviä koulutusvideoita.

Toivomme, että annat meille palautetta tästä materiaalista. Saatuamme riittävästi parannus ja korjausehdotuksia, julkaisemme tästä päivitetyn version.
Linkki palautekyselyyn.

Miksi turvallisesta työskentelystä on tullut entistä tärkeämpää?

Turvallisen työskentelyn merkitys on korostunut muutaman viimeisen vuoden aikana. Taustalta voidaan nostaa esille seuraavat neljä havaintoa:

1) Digitaalisten palveluiden hyödyntäminen on yleistynyt

   - Tuotamme yhä enemmän palveluita digitaaliseen toimintaympäristöön ja käytämme niitä itse yhä enemmän, myös vapaa-ajalla.

2) Koronaviruspandemia on vaikuttanut tapaamme työskennellä digimaailmassa

   - Koronaviruspandemia on muuttanut tapaamme työskennellä nopeammin kuin mikään muu aiempi muutos; erityisesti etätyön käyttäjämäärissä on tapahtunut valtava kasvu. Tietyt muutokset tulevat olemaan pysyviä, myös korona-ajan jälkeen, esimerkiksi etätyön ja käyttöönotettujen uusien palveluiden ja toimintamallien osalta.

- Koronaviruspandemiaa hyödynnetään aktiivisesti tietoverkkorikollisten toteuttamissa huijauskampanjoissa sekä muissa hyökkäyksissä. Muutenkin tietoverkkorikollisten ja valtiollisten toimijoiden aktiivisuus on kasvanut merkittävästi viimeisen vuoden aikana. Meitä käyttäjiä ja meidän käyttämiä ICT-palveluita vastaan hyökätään koko ajan kehittyvien, myös uudenlaisten hyökkäysten avulla. Esimerkiksi saamme nyt huijaus- ja kalasteluviestejä ja yrityksiä puhelimitse (huijauspuhelut), tekstiviesteinä, sähköpostiviesteinä, pikaviesteinä, nettisivuilta ponnahtavina huijausyrityksinä sekä some-alustojen kautta tulevina yrityksinä.

3) Henkilötietojen käsittelyn ja tietoturvallisuuden merkitys on kasvanut

   - 25.5.2018 sovellettavaksi tullut EU:n yleinen tietosuoja-asetus on lisännyt henkilötietojen vaatimustenmukaisen käsittelyn ja tietoturvallisuuden toteuttamisen merkitystä. Meistä jokainen haluaa olla varma siitä, että meidän omia henkilötietoja käsitellään turvallisesti ja luotettavasti ja myös meidän itse täytyy työtehtäviä hoitaessamme huolehtia tästä omalta osaltamme.

4) ICT-palveluissa esiintyvät häiriöt, henkilötietojen tietoturvaloukkaukset ja kyberhyökkäykset ovat yleistyneet

   - Suurimmat digitaalista toimintaamme uhkaavat seikat ovat ICT-toimintaan liittyvät tekniset häiriöt, itse tekemämme inhimilliset virheet sekä tietoverkkorikolliset. Valitettavan useat digimaailman ongelmat johtuvat meistä itsestämme. Etenkin kiireessä virheiden todennäköisyys kasvaa. Valitettavasti tietoverkkorikolliset kehittävät menetelmiään nopeammin kuin pystymme kehittämään suojautumiskeinojamme.

Me kaikki voimme vaikuttaa edellä mainituista kohdista osin kahteen viimeisimpään. Tässä tukimateriaalissa kuvaamme sellaisia hyviä käytäntöjä, joita noudattamalla toimimme vastuullisesti ja vaatimustenmukaisesti, vältämme inhimillisiä virheitä sekä hankaloitamme tietoverkkorikollisten toimintaa.

Tässä esitetyt hyvät käytännöt ovat esimerkkejä, joita jokainen organisaatio voi käyttää mallina oman ohjeistuksen tuottamisessa tai päivittämisessä.

2 TTTT-toimintamalli turvallisen toiminnan mahdollistajana

Tämä tukimateriaali pohjautuu TTTT-toimintamalliin. Se tarkoittaa

Tunnista ja luokittele Tiedot

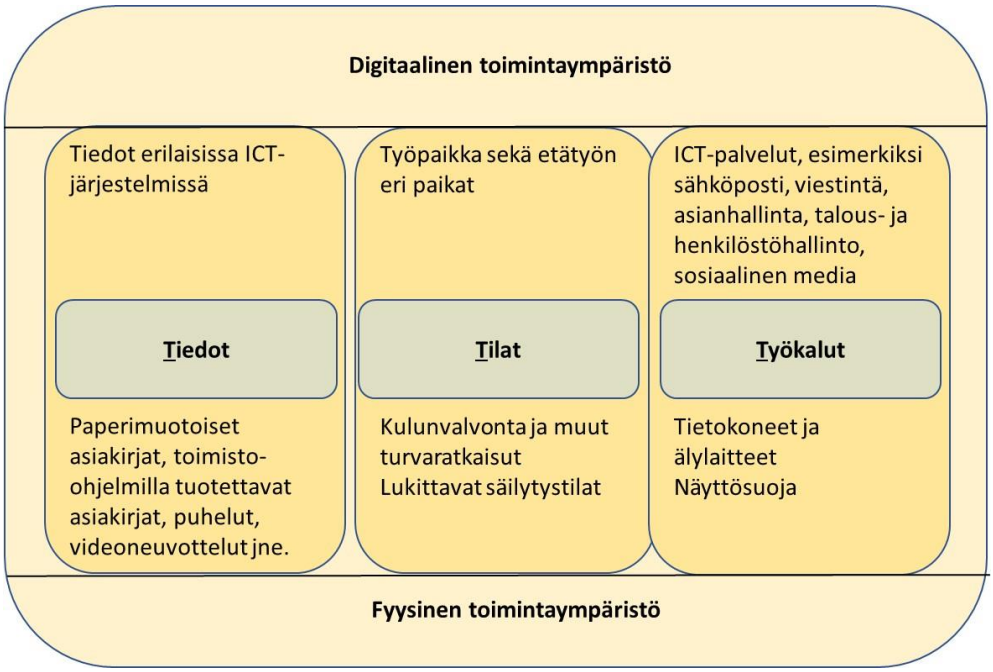
1) jotta voimme toimia turvallisesti ja käsitellä tietoja niille asetettujen vaatimusten mukaisesti, sinun tulee tunnistaa käsittelemiesi tietojen luokka. Tämä määrittää sen, millaisissa tiloissa ja millaisia palveluita käyttäen näitä tietoja voi käsitellä.

tunnista Tilat

2) kun olet määrittänyt käsittelemiesi tietojen luokituksen, sinun tulee tunnistaa, millaisissa fyysisissä (työskentely)tiloissa näitä tietoja on mahdollista käsitellä.

tunnista Työkalut

3) kun olet tunnistanut käsittelemiesi tietojen luokituksen, sinun tulee tietää, millä laitteilla ja millaisissa digitaalisen toimintaympäristön, organisaation omissa tai ulkoisissa, ICT-palveluissa näitä tietoja on mahdollista käsitellä.



Kuva 1. TTTT-toimintamallin avulla voit varmistaa, että käsittelet tietoja turvallisesti, vaatimustenmukaisesti ja huomioit digitaalisen ja fyysisen toimintaympäristön erityispiirteet.

TTTT-mallin lisäksi, ennen kuin toimit, **tarkasta ja pysähdy** vielä kerran varmistamaan, että kaikki näyttäisi olevan oikein. Varmista esimerkiksi ennen sähköpostisi lähettämistä:

1) onko sähköpostissa oikeat vastaanottajat

2) onko viestissä mukana oikea liitetiedosto

3) lähetetäänkö viesti oikealla tavalla, esimerkiksi turvapostilla, jos se lähetetään organisaation ulkopuolelle ja se sisältää henkilötietoja tai salassa pidettäviä tietoja

4) ja esimerkiksi käyttäessäsi some-palveluita, onko some-päivityksessä oleva kuva oikea, eikä siitä paljastu mitään sinne kuulumattomia tietoja, ja onko päivitykseen kytketty (”tägätty”) oikeat henkilöt

2.1 Riskienhallinta on kaiken turvallisen työskentelyn perusta

Kaikki edellä mainitut näkökulmat edellyttävät myös **uhkien tunnistamista ja riskien hallitsemista**. Tietojen tunnistamisen ja luokittelun osalta ei tule ottaa riskejä, vaan niissä tilanteissa, joissa et ole varma tietojen luokittelusta, velvollisuutesi on selvittää ja pyytää tarvittaessa apua. Tilojen käytössä joudut aina tapauskohtaisesti arvioimaan, miten kukin tila soveltuu käsiteltävänä olevien tietojen käsittelyyn. Vastaavasti työkaluja saat käyttää vain sellaisten tietojen käsittelyyn, joihin kyseiset työkalut on tarkoitettu. Et saa esimerkiksi lähettää salassa pidettäviä asiakirjoja tai henkilötietoja organisaatiosi ulkopuolelle, ellet ole muulla tavalla, kuten turvapostilla tai muulla asianmukaisella tavalla huolehtinut tietojen suojaamisesta. Huolehdi myös siitä, että salassa pidettävät tiedot eivät päädy myöskään mihinkään turvattomaan palveluun.

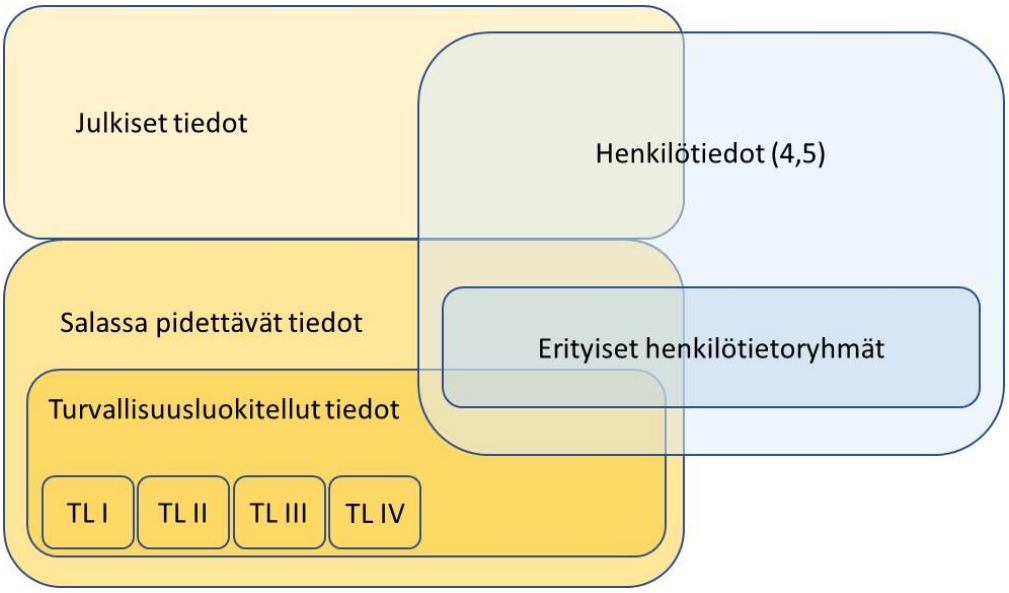
Riskienhallinta pohjautuu riskin toteutumisen todennäköisyyden ja siitä seuraavan vaikutuksen arviointiin. Mitä suurempi todennäköisyys ja erityisesti riskin toteutuessa sillä on vaikutusta toimintaan, sitä isompi vaikutus päätettävänäsi olevalla toimenpiteellä on riskin toteutuessa. Lähdettyäsi työpaikalta – tai kotoasi, mietit, menikö ulko-ovi huonosti kiinni? Todennäköisesti meni, mutta millainen riski siitä syntyy, jos ovi jäi vaikkapa viikonlopuksi auki? Useimmat palaavat takaisin varmistamaan asian – toteuttavat samalla riskienhallintaa. Vaikka et olisi itse sitä tunnistanut, niin toteutat joka päivä valtavan määrän erilaisia päätöksiä, niin työpaikalla kuin arjessa. Mutta kuinka monessa niissä aidosti arvioitu riskejä ja vaikutuksia?

Kaikkien pitää raportoida työtehtävissä havaitsemiaan uhkia tai toteutuneita riskejä ja ilmoittaa niistä organisaation antamien ohjeiden mukaisesti. Turvallisuudesta huolehtiminen on meidän kaikkien yhteinen asia.

3 Tunnista tiedot

Käsittelemiesi tietojen oikeaoppinen tunnistaminen ja luokittelu ovat tärkeitä, koska TTTT-mallin kaksi viimeistä osa-aluetta pohjautuvat siihen, että luokittelu on tapahtunut oikein. Mikäli luokittelet tiedot väärin, se saattaa johtaa tietojen turvattomaan käsittelyyn. Tiedot voivat päätyä sellaisten tahojen haltuun, joilla ei ole niihin oikeutta. Tai väärin luokiteltu tieto voi edellyttää enemmän toimenpiteitä, esimerkiksi jos julkista tietoa käsitellään virheellisesti salassa pidettävänä ja estää täten tiedon hyödyntämistä.

Yleisesti ottaen tietoja luokitellaan henkilötietojen sekä niiden salassapidon mukaisesti. Sisältyykö tietoihin jompaakumpaa? Entä, sisältyykö niihin vielä jotain erityistä? Koskeeko luokittelu koko asiakirjaa vai vain osaa siitä? Kaikissa tapauksista tiedon eheydestä ja saatavuudesta on pidettävä kiinni oikean luokittelun vaatimusten mukaisesti.



Kuva 2. Esimerkkejä tietojen luokittelun eri tasoista. Huomaa, että henkilötiedot voivat olla myös julkisia, mutta tyypillisesti ne ovat salassa pidettäviä.

Kuva 3. Esimerkkejä tietojen julkisuuden luokittelun eri tasoista. Huomaa, turvallisuusluokiteltuja tietoja voidaan luokitella vain valtionhallinnossa ja niille on käytössä tasot I, II, III ja IV. Näistä I ja II tarvitsevat erityisiä tiloja käsittelyyn ja niiden siirtelyyn on erityisiä vaatimuksia.

3.1 Henkilötiedot

Jokaisen meistä tulee kyetä tunnistamaan, mitkä tiedot ovat henkilötietoja ja lisäksi mitkä niistä kuuluvat erityisiin henkilötietoryhmiin. Tästä löytyy kattava ohjeistus Tietosuojavaltuutetun toimiston sivuilta (https://tietosuoja.fi/mika-on-henkilotieto)

”Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. Henkilötietoja ovat sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Henkilö voidaan tunnistaa esimerkiksi nimen, henkilötunnuksen tai jonkin hänelle tunnusomaisen tekijän perusteella.”

Suosittelemme kaikkia julkishallinnon sekä muiden organisaatioiden henkilöstöä suorittamaan verkkokoulutuksen:
Tietosuojan ABC julkishallinnon henkilöstölle 2020

3.2 Erityiset henkilötietoryhmät

Jokaisen meistä tulee myös tunnistaa, mitkä tiedoista kuuluvat erityisiin henkilötietoryhmiin. Näistä on ohjeistettu Tietosuojavaltuutetun toimiston ohjeessa (https://tietosuoja.fi/erityisten-henkilotietoryhmien-kasittely):

Tällaisista tiedoista ilmenee henkilön

1) rotu tai etninen alkuperä
2) poliittisia mielipiteitä
3) uskonnollinen tai filosofinen vakaumus
4) ammattiliiton jäsenyys
5) terveyttä koskevia tietoja
6) seksuaalinen suuntautuminen tai käyttäytyminen
7) geneettisiä ja biometrisia tietoja henkilön tunnistamista varten.

Näitä tietoja on suojeltava erityisen tarkasti, koska niiden käsittely voi aiheuttaa huomattavia riskejä henkilön perusoikeuksille ja -vapauksille.

Näihin kategorioihin kuuluvista tiedoista käsitellään julkisen hallinnon organisaatioissa tyypillisesti määrällisesti eniten terveyttä koskevia tietoja. Lisäksi useat meistä käsittelevät niitä vapaa-ajalla esimerkiksi omaan tai läheisten terveydenhoitoon liittyen.

Terveystietojen käsittelyyn pitää kiinnittää erityistä huomiota, koska tietoverkkorikolliset ovat havainneet niiden korkean markkina-arvon. Saadakseen niitä haltuunsa, he kehittävät uudenlaisia hyökkäyksiä tietojärjestelmiin sekä käyttäjiin kohdistuvia huijauksia.

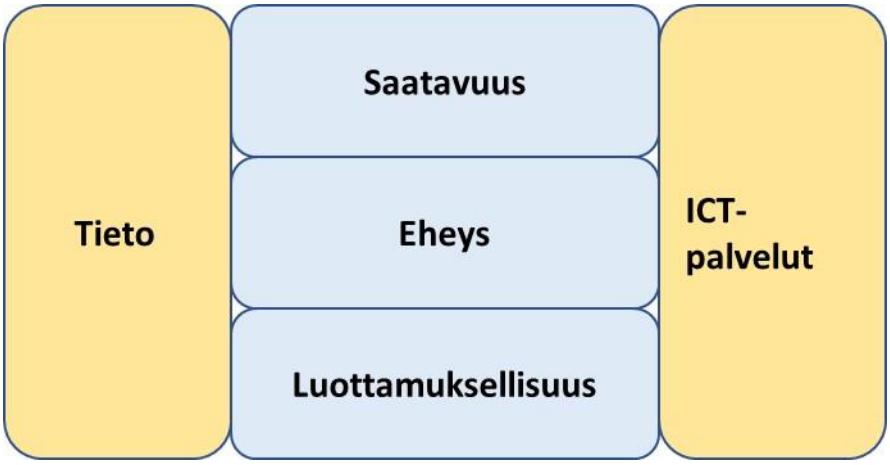
Muista! Aina kun sinulta kysytään henkilötietoja, varmista kuka kysyy, miksi niitä kysytään ja mihin käyttötarkoitukseen – älä luovuta tietoja ennen kuin olet varma siitä, että kyseessä ei ole esimerkiksi huijausyritys. Ole erityisen varovainen sähköpostitse, sms-tekstiviesteistä, pikaviestimistä tulevien tai nettisivuilta ponnahtavien kyselyiden suhteen.

3.3 Julkiset asiakirjat

Kaikki tieto on julkista, ellei se ole lain perusteella salassa pidettävää. Myös henkilötiedot voivat olla julkisia, mutta niitä saa siinäkin tapauksessa käsitellä vain tietosuojalainsäädännön sallimissa puitteissa.

Myös julkisen tiedon käsittelyssä edellytetään tietoturvallisuuden toteuttamista. Tietoturvallisuus kattaa toimenpiteet tiedon **saatavuuden**, **eheyden** ja **luottamuksellisuuden** takaamiseksi. Vaikka julkinen tieto ei edellytä salassapidon, eli luottamuksellisuuden toteuttamista, niin kahdesta muusta tietoturvallisuuden osa-alueesta eli eheydestä ja saatavuudesta tulee kuitenkin aina huolehtia.

Vaikka Suomessa ei ole erikseen määritelty vaatimuksia tiedon eheyden ja saatavuuden takaamiseksi, niitä voidaan määritellä luokittelemalla tietojärjestelmiä niiden sisältämien tietojen toiminnallisen merkityksen ja tietojen kriittisyyden perusteella. Esimerkiksi nettipalvelu, jossa julkaistaan organisaation henkilöstöruokalan julkinen lounaslista, ei ole tiedon eheyden tai palvelun saatavuuden kannalta niin kriittinen kuin palvelu, josta löytyy organisaation toimintaan liittyvissä häiriötilanteissa tarvittavat ohjeet ja yhteystiedot.



Kuva 4. Tietoturvallisuuden avulla huolehditaan tietojen ja niihin liittyvien ICT-palveluiden ja laitteiden saatavuudesta, eheydestä sekä luottamuksellisuudesta.

3.4 Salassa pidettävät asiakirjat

Asiakirjoihin tehtävistä salassapitoa koskevista merkinnöistä säädetään viranomaisten toiminnan julkisuudesta annetun lain 25 §:ssä Salassapito- ja luokitusmerkintä (https://www.finlex.fi/fi/laki/ajantasa/1999/19990621). Jokaisessa julkisen hallinnon organisaatiossa tulee olla ohjeistus ja koulutus siitä, miten tämä luokittelu toteutetaan.

3.5 Turvallisuusluokiteltavat asiakirjat

Turvallisuusluokiteltavista asiakirjoista säädetään Laki julkisen hallinnon tiedonhallinnasta (https://www.finlex.fi/fi/laki/alkup/2019/20190906) 18 § seuraavasti:

”Valtion virastoissa ja laitoksissa toimivien viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan. Turvallisuusluokkaa koskeva merkintä on tehtävä, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2, 5 tai 7–11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.”

Tarkemmat vaatimukset turvallisuusluokitellun tiedon käsittelystä annetaan Valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa. https://www.finlex.fi/fi/laki/alkup/2019/20191101

Tiedonhallintalautakunta on julkaissut tätä koskevan suosituksen 18.1.2021: http://urn.fi/URN:ISBN:978-952-367-500-1

4 Tunnista tilat

Kun olet tunnistanut käsittelemiesi tietojen luokituksen, se vaikuttaa suoraan siihen, millaisissa tiloissa tietoja voi käsitellä. Tässä tukimateriaalissa kuvataan yleisellä tasolla tilojen vaikutusta tietojen käsittelyyn. Jokaisen organisaation tulee itse määrittää tarkemmat ohjeet, joita henkilöstön tulee noudattaa.

Vaikka toimintamme on siirtynyt kasvavassa määrin digitaaliseen toimintaympäristöön, olemme kuitenkin aina läsnä jossakin fyysisessä toimintaympäristössä.

Kuva 5. Tietojenkäsittely on turvallisinta työnantajan käyttöösi tarjoamissa työtiloissa. Mikäli valtionhallinnon organisaatio käsittelee turvallisuusluokiteltavia tietoja, niiden käsittelystä ja tiloista on ohjeistettava erikseen.

4.1 Työpaikka

Työnantajasi on toteuttanut käyttöösi turvalliset työskentelytilat sinulle tarjolla oleviin toimitiloihin. Suojanasi ovat fyysisten turvarakenteiden (seinät, portit, kulunvalvonta, lukitukset, hälytin- ja valvontalaitteet) ohella turvalliset tietoliikenneyhteydet ja niiden turvaratkaisut. Käsittelemiesi tietojen luokituksesta ja organisaatiosi antamista ohjeista riippuen, osaa tiedoista saattaa olla mahdollista käsitellä vain työnantajasi tiloissa. Silloin niiden käsittely ei ole sallittua missään muualla, kuten etätöissä kotona, työmatkalla, toisen organisaation tiloissa tai julkisissa tiloissa.

4.2 Työpaikan turvallisuusluokitellut tilat

Valtionhallinnon organisaatioiden pitää ohjeistaa siitä, millaisissa tiloissa turvallisuusluokiteltuja tietoja on mahdollista käsitellä. Turvallisuusluokitusasetuksen 9 §:n mukaisesti tiedonhallintayksikön on määritettävä fyysisesti suojatut turvallisuusalueet turvallisuusluokiteltujen asiakirjojen käsittelyn ja tietojärjestelmien suojaamiseksi.

Turvallisuusalueita ovat hallinnolliset alueet ja turva-alueet. Näistä on ohjeistettu Tiedonhallintalautakunnan julkaisemassa ”Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä” luvussa ”Asiakirjan käsittelyn ja tietojärjestelmien suojaaminen turvallisuusalueiden avulla”.

4.3 Etätyö

Etätyön merkitys on noussut uuden teknologian tarjoamien mahdollisuuksien myötä; ajasta ja paikasta riippumaton työ tulee yleistymään entisestään 2020-luvulla. Vastaavalla tavalla pystymme hoitamaan yhä enemmän vapaa-aikaan liittyvää asiointia digitaalisten palveluiden avulla.

Perinteisesti etätyö mielletään kotona tehtäväksi työksi. Etätyöllä kuitenkin tarkoitetaan kaikkea työpaikan ulkopuolella tapahtuvaa työskentelyä, oli se sitten kotona, kesämökillä, työmatkalla kotimaassa tai ulkomailla, kahvilassa, asiakkaan tai yhteistyökumppanin tiloissa tapahtuvaa työskentelyä.

Etätöissä toimittaessa tulee ottaa huomioon seuraavat asiat yleisellä tasolla, jokainen organisaatio tyypillisesti tarkentaa näitä ohjeita:

a) Paperimuotoisten tietoaineistojen hallinta

- varmista tietoaineistojen turvallinen kuljettaminen työpaikalta etätyöpaikalle sinulle annettujen ohjeiden mukaisesti
- varmista, että tietoaineistot eivät missään vaiheessa päädy ulkopuolisten haltuun
- varmista, että sekä julkiset että erityisesti henkilötiedot ja mahdolliset salassa pidettävät tiedot säilytetään lukituissa tiloissa
- huolehdi tietojen turvallisesta hävittämisestä organisaation antamien ohjeiden mukaisesti, älä hävitä tietoja itse kotona, vaan toimi prosessin mukaisesti
- varmista tietoaineistojen palauttaminen työpaikalle siinä vaiheessa kuin se on mahdollista

b) ICT-laitteiden ja palveluiden turvallinen käyttö

- huolehdi, että tietokoneen näyttö on sijoitettu siten, että ulkopuoliset henkilöt eivät näe sitä tilan sisä- tai ulkopuolelta
- varmista, että tietoturvasuoja (ns. privacy filter) on käytössä kannettavissa tietokoneissa ja sellaisissa näytöissä, joissa on riskinä, että ulkopuolinen taho saattaa nähdä tietoja. Kannattaa kiinnittää huomiota myös näytön kirkkauteen, sillä liian kirkas näyttö voi tehdä tyhjäksi tietosuojakalvon käyttämisen. Huomaa, että vaikka suoja on käytössä, suoraan takaa katsottuna tiedot voivat silti olla

nähtävissä.

- Pidä aina työnantajan laitteita mukanasi ja älä jätä niitä vartioimattomaan paikkaan.
- Sammuta tietokoneesi työpäivän lopuksi. Näin vaikeutat mahdollisen varkaan pääsemistä käsiksi työaseman tietoihin, erityisesti silloin kun työaseman kovalevy on kryptattu eli salakirjoitettu.

c) Keskustelut

- Puhelimessa puhuttaessa tai osallistuttaessa verkkokokouksiin huomioi muut samassa tilassa olevat henkilöt ja sovita käytävä keskustelu tilanteeseen. Jos paikalla on muita henkilöitä, niin käytä kuulokkeita laitteen oman tai ulkoisen kaiuttimen sijasta. Huomioi äänen kulkeutuminen myös tilan ulkopuolelle.

- jos kotonasi on käytössä ns. älykaiutin tai digitaalinen avustin, se tulee sammuttaa, silloin kuin hoidat työtehtäviä.

d) Henkilötunnisteet

- Säilytä turvallisesti työantajan käyttöösi antamia kulkuavaimia ja henkilökortteja.

- Pidä henkilökortti aina näkyvillä liikkuessasi työpaikallasi, jotta tiedetään, kenellä on oikeus olla tiloissa. Ulkopuolisten kortittomien pitää useimmissa paikoissa ilmoittautua vastaanotossa ja he saavat oman vierailijatunnuksensa. Ilmoita tuntemattomista henkilöistä, joilla ei ole esittää asianmukaista henkilökorttia, äläkä päästä tuntemattomia henkilöitä sisään samalla ovenavauksella!

e) Käytettävän verkon (internet-yhteyden) valinta

Toimiessasi työpaikan tai kotona olevan etätyöpisteen ulkopuolella, ole huolellinen käytettävän internet-yhteyden kanssa. Yleensä työnantajasi tarjoaa käyttöösi VPN-yhteyden, jota käyttämällä tietoliikenneyhteys salataan joko työnantajasi verkkoon tai VPN-palvelun tarjoajan palvelimelle saakka. Sillä vaikeutetaan verkkorikollisten tekemiä hyökkäyksiä sekä salataan tietoliikenneyhteyden kautta kulkeva tieto. Kannettavat tietokoneet käyttävät usein langatonta verkkoa (WLAN / WIFI). On tärkeää tunnistaa, onko langaton verkko avoin vai suojattu. Suojatun langattoman verkon tunnistaa yleensä verkon symbolin vieressä olevasta lukon kuvasta. Se tarkoittaa, että verkon käyttämiseen tarvitaan salasanaa. Jos käytät avointa langatonta verkkoa ilman VPN-yhteyttä, olet alttiina erilaisille verkkorikollisten tekemille hyökkäyksille. Avointa verkkoa turvallisempi tapa on jakaa internet-yhteys tietokoneelle omalta älypuhelimelta. Tällöin tietoliikenneyhteys kulkee suoraan tietoliikenneoperaattorin verkkoon ilman

välillä olevia tunnistamattomia laitteita. Tukiasemakäyttö kuluttaa kuitenkin merkittävästi älylaitteen akkua, joten älylaite kannattaa pitää latauksessa.

4.3.1 Etätyö kotona

Etätyöskentelyyn tarvitaan internet-yhteys, jonka muodostamiseen tarvitaan ”verkkolaite”, joita ovat esimerkiksi reititin, usb-modeemi tai adsl/vdsl/kaapeli/valokuitu-modeemi. Myös älypuhelin voi toimia verkkolaitteena jakaessaan internet-yhteyttä muille laitteille.

Kotiverkon turvallisuuden varmistamiseksi usein riittää, että laitteelle ja sen muodostamalle verkolle on asetettu salasana. Lisäksi tulee varmistaa, että verkkolaite on päivitetty uusimpaan ohjelmistoversioon tai siinä on käytössä automaattiset päivitykset. Lisäksi laitteen hallinnan mahdollistavat oletussalasanat pitää vaihtaa. Näiden tarkistaminen on ohjeistettu verkkolaitteen mukana tulevassa käyttöohjeessa. Jos verkkolaitteen tietoturvallisuudesta ei ole huolehdittu, niin tietoverkkorikolliset voivat käyttää haavoittuvia laitteita esimerkiksi verkkoliikenteen kaappaamiseen tai palvelunestohyökkäysten toteuttamiseen. Huomioi myös edellisessä luvussa esille nostetut käytännöt koskien internet-yhteyden valintaa.

4.3.2 Etätyö julkisissa tiloissa

Julkisissa tiloissa on sallittua ainoastaan julkisten tietojen käsittely, ellei organisaatiosi ole siitä muuta ohjeistanut. ICT-palveluiden lisäksi tämä tulee huomioida myös paperimuotoisen aineiston käsittelyssä sekä keskusteluissa esimerkiksi puhelimessa tai verkkokokouksissa. Julkisissa tiloissa tulee olla huolellinen myös siksi, ettei kukaan ulkopuolinen henkilö pääsisi vaikuttamaan käsiteltävänä olevien julkisten tietojen saatavuuteen tai eheyteen. Tähän sisältyy niin pääsy laitteeseen käsiksi hämäämällä, kuin laitteiden nappaaminen väkivaltaa käyttäen. Kannattaa tunnistaa sellaiset julkiset tiedot, joiden menettäminen tai eheyden muuttuminen, kuten tietojen vääräntäminen, voisi aiheuttaa sinulle tai organisaatioillesi selkeän riskin.

Koska tämä tukimateriaali pohjautuu hyviin käytäntöihin, esimerkiksi tämän – kuten tämän tukimateriaalin muiden kohtien osalta organisaatioilla voi olla omia soveltamisohjeita, joissa turvallisuuttaa parannetaan joillakin lisätoimenpiteillä.

4.3.3 Etätyö kotimaan työmatkalla

Kotimaan työmatkoilla pitää huolehtia ennen kaikkea mukana kulkevien tietoaineistojen ja ICT-laitteiden turvallisuudesta. Niitä ei saa päästää matkan aikana näkyvistä, esimerkiksi sijoittamalla ruumaan lentokoneissa tai linja-autoissa.

Jos saat matkallasi esimerkiksi liikelahjoja, jotka voidaan kytkeä työasemasi USB-porttiin tai langattomaan WLAN/WIFI-verkkoon, niitä saatetaan käyttää haittaohjelmien levittämiseen tai tietojen keräämiseen. Siitä syystä saatuja USB-muistitikkuja, internet-verkkoon kytkettäviä laitteita, varavirtapankkeja tai tuulettimia ei kannata liittää työasemaasi, työpuhelimeesi tai langattomaan verkkoosi.

4.3.4 Etätyö ulkomaan työmatkalla ja ulkomailla

Ulkomailla tapahtuvassa työskentelyssä tulee ottaa huomioon kaikki samat uhat ja ohjeet kuin Suomessa työskenneltäessä. Sen lisäksi, maasta vaihdellen, tulee ottaa huomioon muita turvallisuuteen liittyviä seikkoja. Saat lisätietoa tietoaineistojen käsittelystä tai päätelaitteiden käyttämisestä ulkomailla organisaatiosi omista ohjeista.

Eräs hyvä käytäntö on, että ulkomaille matkustaessaan henkilö saa käyttöönsä pelkästään matkakäyttöön tarkoitetun tietokoneen ja älypuhelimen. Niistä on karsittu pois kaikki turhat toiminnot ja muutenkin pyritty vahvistamaan laitteiden turvallisuutta. Matkalta palattaessa kyseiset laitteet palautetaan ja ne asennetaan uudelleen ennen seuraava käyttökertaa. Tällä pienennetään myös riskiä, joka syntyy, jos matkan aikana laitteiden tietoturvallisuus onnistutaan murtamaan. Älä siis liitä matkakonetta suoraan työpaikkasi verkkoon palattuasi, jottei mitään siirry sen kautta verkon suojausten ohi.

Mikäli osallistut johonkin kansainväliseen verkkoseminaariin tai vastaavaan tilaisuuteen (myös Suomesta etänä), ole erityisen varovainen, jos saat tällaisen tilaisuuden jälkeen sosiaalisen median kautta verkostoitumispyyntöjä tai muita yhteydenottoja. Tällaisten tilaisuuksien osallistujalistat ovat usein julkisia, joka tarjoaa väärinkäyttäjille helpon tavan lähestyä sinua ja pyrkiä verkostoihisi.

Ulkomailla liikkuessasi kannattaa myös käyttää sosiaalista mediaa maltillisesti. Esimerkiksi tiedot siitä, missä olet ja minne olet menossa sekä mikä on matkasi tarkoitus, voivat olla verkkorikolliselle tai muille väärinkäyttäjille hyödyllisiä tietoja.

Ulkomailla liikkuessa kannattaa käyttää aina VPN-yhteyttä, mikäli sellaisen käyttäminen on maassa mahdollista. Jos aiot käyttää matkapuhelinyhteyttä ulkomailla, erityisesti EU-alueen ulkopuolella, kannattaa tutustua ensin työantajan käyttämän operaattorin hinnastoon. Useissa maissa tiedonsiirto ei kuulu liittymän perusmaksuun, joten yritä välttää yllättäviä puhelinlaskuja työnantajalle.

Organisaatio voi hyödyntää alla mainittua VAHTI-ohjetta ulkomaan ohjeistuksensa laadinnassa:

VAHTI 4/2013 Henkilöstön tietoturvaohjeen tukimateriaali - 9. liite 6 tietoturvallisuuden huomioiminen ulkomaille matkustettaessa tai siellä työskenneltäessä.

https://www.suomidigi.fi/vahti-42013-henkiloston-tietoturvaohjeen-uusi-tukimateriaali-9-liite-6-tietoturvallisuuden-huomioiminen-ulkomaille-matkustettaessa-tai-siella-tyoskennelta-essa

5 Tunnista käytettävissä olevat laitteet ja työkalut

TTTT-mallin viimeinen osa-alue koskee käytettävissä olevia työkaluja, siis laitteita ja palveluita. Käytännössä tietoaineistojen luokittelu määrää suoraan sen, millaisia laitteita ja palveluita niiden käsittelyssä voi käyttää. Organisaatiosi antamista ohjeista ei tule poiketa.

Voit soveltaa tässä kuvattuja käytäntöjä työtehtävien hoitamisen ohella myös vapaa-ajan käytössä olevissa laitteissa ja palveluissa.

5.1 Työnantajan käyttöösi tarjoamat ICT-laitteet

5.1.1 Tietokoneet

Henkilöstön käyttöön tarkoitetut päätelaitteet, kuten tietokoneet ja älypuhelimet, on tarkoitettu vain oman henkilöstön käyttöön. Niitä eivät saa käyttää ketkään ulkopuoliset, edes perheenjäsenet.

Lähtökohtana voidaan pitää sitä, että työtehtävät tulisi aina tehdä työnantajan käyttöösi antamilla laitteilla. Jos työnantajasi sallii, julkisen tiedon käsittely muilla kuin työnantajan laitteilla on mahdollista. Muun kuin julkisen tiedon käsittelyä henkilökohtaisessa omistuksessa olevalla laitteella ei voida pitää suositeltavana, koska laitteiden kautta tiedot saattavat päätyä huomaamatta ei-toivottuun paikkaan. Esimerkiksi joidenkin laitevalmistajien pilvessä sijaitsevat varmuuskopiopalvelut tai muut vapaa-ajan laitteessa käytössä olevat palvelut saattavat sijaita EU-alueen ulkopuolella, jolloin niihin ei saisi päätyä työtehtäviin liittyviä henkilötietoja hallitsemattomasti. Näihin palveluihin saattavat päästä käsiksi myös ulkomaisten tiedustelupalveluiden edustajat kansallisen lainsäädännön mahdollistamana. Tämän takia salassa pidettäviä tietoja ei henkilökohtaisessa omistuksessa olevalla laitteella pidä käsitellä.

On tärkeää, että kaikkiin päätelaitteesiin on asetettu salasana, pin-koodi tai biometrinen tunniste, jonka avulla laite aukeaa. Päätelaitteet tulee myös asettaa lukittumaan automaattisesti, kun työskentely niillä loppuu. Näin laitteet pysyvät lukittuina aina kun niitä ei käytetä.

Päätelaitteissa tulee huolehtia myös siitä, että niiden käyttöjärjestelmät ja ohjelmistot ovat ajan tasalla. Usein työnantajan laitteissa päivitykset asennetaan keskitetysti, jolloin käyttäjän vastuulle jää huolehtia siitä, että päätelaitteen ehdottamat automaattiset päivitykset suoritetaan. Tarvittaessa laite tulee käynnistää uudelleen päivitysten viimeistelemiseksi heti kun se on mahdollista. Huolehdi päivityksistä myös omissa vapaa-ajan laitteissasi.

5.1.2 Mobiililaitteet

Tietokoneen tietoturvallisuudesta huolehtiminen on monille jo automaattista. Myös puhelimen tai älylaitteen tietoturvallisuudesta huolehtiminen on yhtä tärkeää, sillä puhelimesta on usein pääsy samoihin tietoihin ja palveluihin, kuten sähköpostiin ja kalenteriin. Haittaohjelman tartuttama puhelin toimii myös rikolliselle hyvänä apuvälineenä uhrin sijainnin paikantamiseen, salakuunteluun tai salaa kuvaamiseen.

Voit parantaa puhelimesi tai älylaitteesi tietoturvallisuutta muutamalla yksinkertaisella toimenpiteellä:

1. Lue sovellusten käyttöehdot

Hyväksyitkö uutta sovellusta asentaessasi käyttöehdot lukematta niitä? Käyttöehdoissa tai tietosuojaselosteessa kerrotaan, mitä henkilötietoja sovellus käyttäjästään kerää, mihin tarkoitukseen niitä käytetään ja mille tahoille niitä välitetään. Lisäksi niissä kerrotaan käyttäjän oikeuksista omiin henkilötietoihinsa sekä kuinka kauan henkilötietoja säilytetään esimerkiksi tilin poistamisen jälkeen.

2. Päivitä laitteen ohjelmisto

Tietokoneessa tai puhelimessa käyttöjärjestelmä on laitteen aivot, joita korjataan ja parannellaan päivityksillä. Ne voivat korjata aiemmassa versiossa olleita virheitä tai lisätä laitteeseen uusia ominaisuuksia. Käyttöjärjestelmän päivittäminen on suositeltavaa, sillä vanhentuneeseen ohjelmistoon on voinut jäädä virheitä. Ne voivat sisältää haavoittuvuuksia, joiden avulla älypuhelin on mahdollista ottaa haltuun haittaohjelmaa hyödyntäen. Lisäksi on suositeltavaa kytkeä päälle ominaisuus, jolla älypuhelin päivittää käyttöjärjestelmän automaattisesti.

3. Päivitä sovellukset

Käyttöjärjestelmän lisäksi myös älypuhelimeen asennetut sovellukset pitää päivittää. Niiden ohjelmistovirheet voivat pahimmillaan aiheuttaa ulkopuolisen pääsyn sovelluksen (tai puhelimen) tietoihin. Puhelimen asetuksista voi määrittää sen, että puhelin päivittää sovellukset automaattisesti.

4.Tarkista sovelluksien oikeudet

Uutta sovellusta käyttöön otettaessa kysytään, mitä puhelimen toiminnoista sovellus voi käyttää tai mihin tietosisältöihin sillä on käyttöoikeus, esimerkiksi valokuviin ja tiedostoihin. Tässä kannattaa olla tarkkana ja antaa sovellukselle ainoastaan ne oikeudet, jotka ovat välttämättömiä sen käyttötarkoituksiin. Navigointisovellukselle ei tarvitse antaa oikeuksia käyttää puhelimen kuvia tai kuvankäsittelysovelluksella ei ole tarvetta käyttää puhelimen mikrofonia. Sovellusten oikeuksia on mahdollista muuttaa puhelimen asetuksista.

Jos sovellus haluaa käyttää laitteen kameraa tai mikrofonia eikä löydy selkeää perustetta, niin käyttö kannattaa estää sovelluksen asentamisen jälkeen.

5. Ole huolellinen USB-liityntää käyttäviä laitteiden kanssa

Tietokoneen USB-portin välityksellä siirtyy virran lisäksi mobiililaitteelle myös dataa, joten sen välityksellä saattaa levitä haittaohjelmia.

Hyvä yleissääntö on, että käytät työnantajan laitteiden kanssa ainoastaan työnantajan tarjoamia USB-laitteita. Muista tämä erityisesti muistitikkujen kanssa, sillä henkilökohtaisessa käytössä olevien tikkujen välityksellä työnantajan työasemalle saattaa siirtyä haittaohjelmia.

5.2 Työantajan käyttöösi tarjoamat palvelut

Työantajasi tarjoaa käyttöösi ICT-palveluita työtehtävien hoitamiseen. Velvollisuutesi on käyttää niitä annettujen ohjeiden mukaisesti.

5.2.1 Palveluihin kirjautuminen

Palveluihin kirjautuminen on yksi turvallisuuden kannalta kriittisimmistä digitaalisen palvelun käytön vaiheista. Seuraavaksi esitellään yleisimmät palveluiden kirjautumistavat ja niihin liittyviä hyviä käytäntöjä.

Verkkopalveluita käytettäessä hyvän salasanan merkitys korostuu, koska samoja tunnuksia voidaan käyttää useamman palvelun hallintaan. Esimerkiksi Facebook-, Apple-, Google- tai Office 365 -tilien avulla voidaan kirjautua samoilla tunnuksilla useisiin eri palveluihin, kuten kalenteriin, tallennustilaan ja sähköpostiin sekä mahdollisesti myös kolmannen osapuolen palveluihin. Jos salasanan päätyy vääriin käsiin, niin ulkopuolinen saa pääsyn kaikkiin näihin palveluihin ja niihin tallennettuihin tietoihin. Työtehtäviin liittyviin palveluihin ei tule tunnistautua käyttäen edellä mainittuja sosiaalisen median palveluita, vaan jokaiseen palveluun tulee kirjautua työsähköpostiosoitteella tai muulla työnantajan käyttöösi tarjoamalla tunnistautumismenetelmällä.

Sähköpostipalvelun salasanan kanssa tulee olla erityisen huolellinen, sillä useisiin palveluihin kirjaudutaan käyttäen sähköpostiosoitetta käyttäjätunnuksena. Usean palvelun salasana voidaan vaihtaa sähköpostiosoitteen avulla, joten sähköpostitilin ollessa väärissä käsissä, sen kautta voidaan päästä käsiksi myös muihin palveluihin.

5.2.2 Turvallinen salasanan hallinta

Digitaalisessa maailmassa salasana vastaa avainta fyysisessä maailmassa. Se ei saa päätyä vääriin käsiin. Avainta ei anneta ulkopuolisille, joten samaa huolellisuutta ja varovaisuutta tulee noudattaa salasanojen kanssa.

Hyvän salasanan tulee olla:

1. **Muistettava**

Salasanan yksi tärkeimmistä ominaisuuksista on se, että se on muistettava. Jos salasana ei ole muistettava, tulee se helposti kirjoitettua ylös muistilapulle. Tällöin se voi joutua ulkopuolisten käsiin. Mikäli kirjoitat salasanan paperille tai tallennat tietokoneella tai älylaitteelle, tallenna se siten, että salasanasta ei käy suoraan ilmi, mihin palveluun se on tarkoitettu sekä voit tarvittaessa lisätä sen perään tai alkuun lisämerkkejä sen väärinkäytön estämiseksi.

2. **Pitkä**

Nykytiedon mukaan salasanan pituus on tärkeämpää kuin sen monimutkaisuus, eli esimerkiksi sen sisältämien erikoismerkkien määrä. Tietokoneiden laskentatehon kasvaessa myös verkkorikollisten mahdollisuudet selvittää salasana palveluista

tietomurron avulla saatujen salasanojen avulla kasvavat. Salasanan pituuden kasvaessa myös sen murtamiseen tarvittava aika kasvaa. Hyvä tapa on muodostaa salasanan sijaan salasanalause. Lauseen arvattavuutta voidaan vaikeuttaa myös käyttämällä murresanoja tai vaihtamalla esimerkiksi kirjaimia numeroiksi. Tärkeää on kuitenkin huolehtia siitä, että salasanan muistettavuus ei kärsi.

3. Ainutkertainen

Verkkorikolliset keräävät ja julkaisevat murrettujen palveluiden salasanoja ja käyttäjätunnuksia, ja yrittävät niiden avulla murtautua toisiin palveluihin. Tästä syystä samaa salasanaa ei saa käyttää eri palveluissa.

Voit hakea inspiraatiota hyvien salasanojen keksimiseen Traficomin Pidempi parempi -kampanjasivustolta osoitteessa: https://pidempiparempi.fi/

Biometrinen tunniste

Biometrisellä tunnisteella tarkoitetaan ihmisen fysiologiaan perustuvaa yksilöivää tunnistamista. Tunnisteina voidaan käyttää esimerkiksi sormenjälkeä tai kasvokuvaa. Näihin käytettävien laitteiden varmuus vaihtelee vielä, eikä näitä pitäisi käyttää ainoana suojana. Vapaa-ajan laitteelle annettua sormenjälkeä ei myöskään pitäisi käyttää työlaitteessa.

Kaksi- tai muu monivaiheinen tunnistus

Joissakin työnantajan tai vapaa-ajan palveluissa on mahdollista käyttää kaksi- tai monivaiheista tunnistusta. Silloin palvelu varmistaa käyttäjän identiteetin kahdessa vaiheessa. Ensimmäinen vaihe on palvelun kiinteän salasanan kysyminen ja toinen vaihe voi olla matkapuhelimeen lähetetyn numerosarjan syöttäminen tai erillisen sovellukseen tuleva hyväksymispyyntö. Kaksivaiheinen tunnistaminen varmistaa, että ulkopuoliset eivät pääse käyttämään palvelua, vaikka he olisivatkin saaneet haltuunsa palvelun salasanan. Jos palvelussa on mahdollista käyttää kaksivaiheista tunnistusta, on sen käyttö erityisen suositeltavaa.

Salasanan hallintaohjelmisto

Salasanojen hallintaohjelma on sovellus, johon on mahdollista tallentaa eri palveluiden salasanat. Se mahdollistaa ainutkertaiset, laadultaan korkeatasoiset salasanat. Ohjelma huolehtii automaattisesti salasanan syöttämisestä, kun jokin verkkopalvelu sitä kysyy. Tällaisen ohjelman etuna on se, että käyttäjän ei tarvitse muistaa kuin yksi salasana ja sovellus muistaa loput. Riskinä on se, että jos hallintaohjelman salasana päätyy vääriin käsiin, päätyvät myös siihen tallennetut salasanat. Jos työnantajasi tarjoaa salasanan hallintaohjelmiston käyttöösi, on sen käyttäminen suositeltavaa. Huolehdi tällöin erityisellä huolella tämän hallintaohjelman salasanasta, jonka takana kaikki muut salasanat ovat.

5.2.3 Sähköposti ja turvaposti

Useimmissa organisaatioissa voi sisäisesti käsitellä salassa pidettäviä ja henkilötietoja sisältäviä tietoja sähköpostin välityksellä, kun sähköposti ei poistu organisaation ulkopuoliseen osoitteeseen (eli pysyy palvelimella). Tutustu oman organisaatiosi ohjeistukseen.

Lisäksi usein on käytössä turvapostipalvelu, joka mahdollistaa salassa pidettävien tai henkilötietojen lähettämisen organisaation ulkopuolisille vastaanottajille sekä tarvittaessa organisaation sisällä, mikäli organisaation antama ohjeistus sitä edellyttää.

Sähköpostia lähetettäessä tulee kiinnittää huomiota kenttään, johon syötetään vastaanottajan sähköpostiosoite. Yleensä vaihtoehdot ovat vastaanottaja (to), kopio (cc) ja piilokopio (bcc). Joissain sähköpostiohjelmissa (esimerkiksi Outlook) piilokopiovaihtoehto voi olla piilotettuna. Jos käytät vastaanottaja ja kopiokenttiä, kaikkien vastaanottajien sähköpostiosoitteet näkyvät kaikille vastaanottajille. Tämä tulee ottaa huomioon erityisesti lähetettäessä sähköpostia suurella jakelulla tai sellaiseen viestiin vastattaessa; ole huolellinen, haluatko vastata vain viestin lähettäjälle vai kaikille viestin saaneille.

Piilokopiokenttää käytettäessä näyttää siltä, kuin sähköpostin saaja olisi sen ainoa vastaanottaja, vaikka viesti on voitu lähettää suurelle vastaanottajajoukolle.

Usein sähköpostiohjelmat ehdottavat viestin vastaanottajaa automaattisesti kirjoittamasi perusteella. Ole tarkkana, että valitset ehdotuksista tarkoittamasi vaihtoehdon. Joissain ohjelmissa ehdotuksia voidaan poistaa listalta napauttamalla hiirellä nimen kohdalla olevaa rastia.

Kannattaa kiinnittää huomiota lähettäjän sähköpostiosoitteeseen, sillä se on helppo väärentää. Lisäksi käyttäjää voidaan huijata perustamalla sähköpostiosoite, joka sisältää ylimääräisiä merkkejä tai jossa pieni L-kirjain on korvattu isolla I-kirjaimella. Mitä tärkeämmästä viestistä on kyse, sitä tärkeämpää on varmistaa, että vastaanottajan osoite on varmasti oikea ja kirjoitettu oikein.

Sähköpostin sisältämät liitetiedostot ovat yksi tapa levittää haittaohjelmia. Suhtaudu siksi epäluuloisesti kaikkiin liitteisiin, jotka tulevat tuntemattomalta lähettäjältä. Haittaohjelmia voivat sisältää sellaiset Microsoft Office-ohjelmien liitetiedostot, jotka vaativat avautuessaan ns. makrojen sallimista. Vastaa makroja koskevaan kysymykseen aina kieltävästi ja ota yhteys organisaatiosi ICT-tukipalveluun.

Sähköpostilla lähetetään huijauksia ja niiden avulla myös kalastellaan kirjautumistietoja, kuten salasanoja. Huijaussähkön lähettäjätiedot saattavat näyttää täsmälleen samalta, kuin alkuperäinen sähköpostiosoite. Kuitenkin sähköpostissa oleva linkki, jonka avulla esimerkiksi pyydetään tarkistamaan omat tiedot, sisältää jonkin poikkeavan merkin. Tarkoituksena on ohjata vastaanottaja oikealta näyttävälle, mutta väärennetylle sivustolle, joka sijaitsee aivan eri internet-osoitteessa. Tälle sivustolle syötetyt käyttäjätunnukset ja salasanat päätyvät verkkorikollisen käsiin. Jos viestin linkki epäilyttää, se kannattaa unohtaa ja tarkastaa omat tiedot kirjautumalla suoraan palvelun tarjoajan aidon sivun kautta.

5.2.4 Kalenteri

Kalentereiden sisällöt ovat organisaatiossa usein koko henkilöstön nähtävillä. Siksi kalenteritapahtumiin ei tule liittää salassa pidettäviä tai henkilötietoja eikä niitä sisältäviä tiedostoja. Henkilötiedoista kalenterimerkintään saa liittää ainoastaan kokoukseen kutsuttavien henkilöiden sähköpostiosoitteet.

5.2.5 Pikaviestimet

Oletuksena pikaviestimiä tulee käyttää ainoastaan julkisen tiedon välittämiseen. Osa pikaviestintäsovelluksista on rajoitettu käytettäväksi vain vapaa-ajalla, jolloin niiden käyttäminen esimerkiksi työtehtävien hoitamiseen on käyttöehtojen vastaista. Yksi mahdollinen käyttötapa on käyttää pikaviestiä herätteen lähettämiseen siitä, että vastaanottaja on saanut tärkeän sähköpostiviestin. Tällöin varsinainen viestintä tapahtuu turvallisemmassa toimintaympäristössä. Osa organisaatioista on saattanut toteuttaa henkilöstön käyttöön sellaisen pikaviestipalvelun, esimerkiksi Skype tai vastaavan palvelun, joka mahdollistaa myös salassa pidettävän tiedon ja henkilötietojen käsittelyn.

5.2.6 Verkkokokouspalvelut

Pikaviestimien lisäksi myös verkkokokouspalveluissa tulee olla huolellinen siinä, millaisia tietoja kokouksessa on mahdollista käsitellä ja millaisia tietoja palveluun saa tallentaa.

Huolehdi siitä, että henkilötietoja tai salassa pidettäviä tietoja ei ole esimerkiksi kameran näkökentässä, josta ne näkyvät muille kokouksessa oleville.

5.2.7 Varmuuskopiointi

Työaseman tietojen varmuuskopiointi on erityisen tärkeää. Se saattaa auttaa tilanteissa, joissa kiintolevy hajoaa tai kiristyshaittaohjelma lukitsee ja salaa työaseman tiedot. Jos työasemaan tarttuu haittaohjelma, varmuuskopion avulla se voidaan palauttaa aiempaan tilaan. Selvitä miten varmuuskopiointi on organisaatiossasi toteutettu. Joskus esimerkiksi ainoastaan tietty tietokoneellasi oleva kansiorakenne varmuuskopioidaan. Huolehdi myös vapaa-ajan älylaitteiden tietojen varmuuskopioinnista, esimerkiksi valokuvien osalta.

5.3 Sosiaalinen media

Sosiaalisesta mediasta on tullut yhä useamman organisaation lähes reaaliajassa toimiva työkalu, jota hyödynnetään ajankohtaisten tapahtumien seurantaan, verkostoitumiseen, oman asiantuntemuksen kasvattamiseen ja työtehtäviin liittyvien asioiden viestimiseen.

Sosiaalinen media tarjoaa oikein hyödynnettynä loistavia mahdollisuuksia, mutta vastaavasti sen käyttöön liittyy muutama erityinen uhka, jotka tulee ottaa huomioon.

- Käyttäjä saattaa jakaa tai lähettää palveluun vahingossa salassa pidettäviä tietoja. Mikäli palvelu on ulkomailla tai kolmannen osapuolen ylläpitämä, saattaa

aineiston poistaminen olla mahdotonta tai se kestää niin kauan, että tieto ehtii vuotaa ja levitä myös muualle Internet-verkon palveluihin, jolloin tietoaineisto jää nettiin ”ikuisesti”.

- Käyttäjä saattaa tiedostamattaan aiheuttaa tietovuodon. Vaikka hänen yksittäiset viestinsä eivät muodostakaan uhkaa, niin keräämällä yhteen eri palveluiden tai pidemmän aikajakson tietoja, saadaan muodostettua sellainen kokonaiskuva, joka johtaa luottamuksellisen tiedon paljastumiseen.

- Myös toinen henkilö saattaa palveluun lähettämissään viesteissä, valokuvissa tai videotiedostoissa paljastaa tahattomasti käyttäjää tai organisaatiota koskevia luottamuksellisia tietoja. Siksi kannattaa aina tarkistaa kaikki sellaiset viestit ja ilmoitukset, joihin sinut on kytketty (”tägätty”).

12 kohdan tarkistuslista sosiaaliseen median turvalliseen käyttöön:

1. Selvitä ja noudata organisaatiosi sosiaalisen median käyttöpolitiikkaa, jossa on yleensä myös ohjeistettu tietoturvallisesta käyttäytymisestä.

2. Ole erityisen varovainen avatessasi sellaisia sinulle kohdistettuja viestejä, joissa varoitellaan tietoturva-asioista ja pyydetään suojautumaan erilaisilta uhkilta napauttamalla viestissä olevaa linkkiä. Ole varovainen, vaikka tällainen viesti tulisi henkilöltä, johon luotat ja jonka tunnet hyvin. Ota yhteyttä kyseiseen henkilöön vaikkapa puhelimella tai muulla viestintäkanavalla ja varmista viestin aitous. Voit myös netistä hakea lisätietoa kyseisestä varoituksesta tai siihen liittyvästä mahdollisesta huijauksesta. Samoin suhtaudu erittäin suurella varauksella kaikkiin sinulle tuleviin ”aivan liian halpaa tai hyvää ollakseen totta” viesteihin. Ne kannattaa jättää avaamatta ja ainakin olla napauttamatta linkkiä.

3. Jos epäilet, että olet joutunut huijatuksi tai hyökkäyksen kohteeksi, älä epäröi pyytää apua. Ilmoita ehdottomasti asiasta oman organisaatiosi ohjeiden mukaisesti. Älä jätä myöskään vapaa-ajalla tekemättä asiasta rikosilmoitusta, vaikka taloudellinen menetys saattaa osaltasi jäädä vaatimattomaksi.

4. Jos mainitset sosiaalisen median palvelun henkilöprofiilissasi työnantajasi, esiinnyt tällöin organisaatiosi edustajana. Muutenkin, jos käsittelet palvelussa työasioita, toimit tällöin organisaatiosi edustajana. Muista käyttäytyä sen mukaisesti! Mikäli toimit somessa yrityksesi edustajana, voit myös joutua yritykseen kohdistuvan pitkittyneenkin purkauksen kohteeksi. Varmista työnantajasi kanssa menettelyt etukäteen näiden käsittelyssä. Vinkkejä vihapuhetta kohtaan löytyy mm. https://valtiolla.fi/tukimateriaali-auttaa-kasittelemaan-tyossa-kohdattavaa-vihapuhetta/

5. Varo syöttämästä liian henkilökohtaista tai yksityiskohtaista tietoa, valokuvia tai muuta materiaalia itsestäsi, läheisistäsi tai organisaatiostasi. Huomaa, että palvelun tarjoaja tai muu henkilö verkostossasi voi hyödyntää profiiliisi syöttämiäsi tietoja laajasti. Tutustu käyttämiesi palveluiden sopimusehtoihin.

6. Tarkista käyttäjäprofiilin yksityisyyden suojaa koskevat asetukset ja muuta niitä tarvittaessa siten, että tietosi eivät leviä laajemmalle kuin haluamallesi käyttäjäjoukolle. Voit myös pyrkiä rajoittamaan yksittäisten viestien näkyvyyttä.

7. Kunnioita perheesi ja ystäviesi suhtautumista sosiaalisiin medioihin. Vaikka olisit itse niistä innostunut, eivät kaikki sitä kuitenkaan ole. Jos kanssaihmisesi eivät halua sinun laittavan heistä kuvia tai tietoa sosiaaliseen mediaan, noudata heidän toiveitaan. Älä myöskään salli minkään (sosiaalisen median) palvelun ladata esimerkiksi älypuhelimesi yhteystieto-osoitteistoa palveluun, ellei organisaatiosi ohjeistus sitä salli. Harkitse myös tätä vapaa-ajan laitteidesi osalta, luovutatko kaikkien puhelimellasi olevien yhteystiedot palveluun, jos et välttämättä tiedä varmuudella, miten se näitä tietoja käsittelee ja hyödyntää.

8. Ole varovainen, kun sinulle tuntemattomat henkilöt haluavat verkostoitua kanssasi. Älä luota pelkästään siihen, että joku muu verkostossasi oleva on kyseisen henkilön jo hyväksynyt.

9. Älä käsittele salassa pidettäviä tai henkilötietoja sosiaalisessa mediassa tai niiden yksityisviesteissä. Muista, että palvelun ylläpitäjät pääsevät käsiksi

kaikkeen palveluun talletettuun, myös vain keskustelun osapuolten väliseksi tarkoitettuun tietoon.

10. Ennen kuin jaat tietoa sosiaalisessa mediassa edelleen, tarkista sen sisältö. Älä luota pelkkään viestin otsikkoon. Ennen kuin jaat sosiaalisessa mediassa muiden tuottamaa tietoa, varmista, että olet lukenut sen ja tiedät mitä kokonaisuus pitää sisällään ja mikä on viestin tarkoitus. Kannattaa myös ilmoittaa, jaatko kyseistä tietoa, koska olet samaa mieltä vai koska haluat nostaa esiin jotain omasta näkökulmastasi poikkeavaa tietoa. Samoin kannattaa arvioida ennakolta, millaisia reaktioita viesti saattaa herättää ja osin varautua palautteeseen. Erityisesti Twitter on herkkä ”leimahtamaan”.

11. Jos olet epävarma tiedon aitoudesta, on hyvä tarkistaa, kerrotaanko asiasta myös muissa uutislähteissä. Jos siitä ei ole mainintaa muissa tiedotusvälineissä, uutisen todenperäisyyttä voi epäillä ja on syytä harkita tarkkaan, kannattaako viestiä levittää eteenpäin.

12. Pyri tunnistamaan, kun sinuun pyritään vaikuttamaan. Kiireessä emme pysty niin helposti tunnistamaan esimerkiksi meihin kohdistettua piiloviestintää tai muita vaikuttamiskeinoja. Niiden avulla saatetaan pyrkiä vaikuttamaan tunteisiisi, ajatuksiisi, asenteisiisi, päätöksiisi ja tätä kautta käyttäytymiseesi.

5. Miten voin oppia lisää?

Nyt, luettuasi tämän tukimateriaalin ja toteuttamalla tässä esitettyjä hyviä käytäntöjä, omaat hyvät perusteet turvalliselle työskentelylle. Voit opiskella lisää seuraavista Digiturvallinen elämä verkkokoulutuksista:

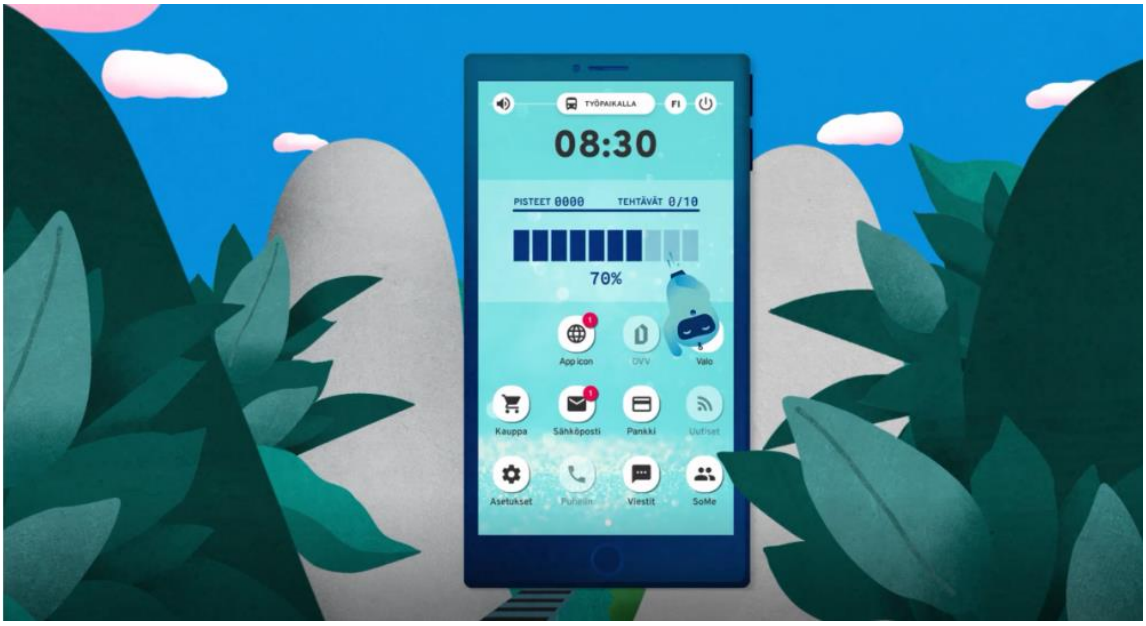
Digiturvallinen työelämä
https://www.eoppiva.fi/koulutukset/digiturvallinen-tyoelama/

Toimi turvallisesti digimaailmassa
https://www.eoppiva.fi/koulutukset/toimi-turvallisesti-digimaailmassa/

Digiturvallisuus kuntien luottamushenkilöille

https://www.eoppiva.fi/koulutukset/digiturvallisuus-kuntien-luottamushenkiloille/

Lisäksi voit harjoitella ja kerrata oppimaasi asentamalla käyttämääsi älypuhelimeen tai tablettiin sovelluskaupasta Digi- ja väestötietoviraston tuottaman **Digiturvallinen elämä -pelin**. Sen läpi pelaamiseen kuluu aikaa noin tunti. Peliin julkaistaan vuonna 2021 yksi päivityspaketti.



Kuva 6. Digiturvallinen elämä opettaa sinulle, kuinka tulee toimia turvallisesti digimaailmassa harjoittelemalla eteesi tulevia uhkia kuvitteellisen Tyrskylän kunnan työntekijänä.