DIGI- JA VÄESTÖTIETO-VIRASTO

TTTT-modellen för säkert arbete

VAHTI-god praxis stödmaterial

3.5.2021

Tfn **0295 536 000** (växel) | Kontaktuppgifter, se **www.dvv.fi**

Hantering av dokument

Ägare	Kimmo Rousku, Myndigheten för digitalisering och befolkningsdata
Upprättat av	Juha Kirves, Kimmo Rousku
Granskat av	VAHTI-sekretariatet
Godkänt av	VAHTI-sekretariatet

Versionshantering

version nr	åtgärder	datum/person
0.42	Första råvaran	18.11.2021 KR, JK
0.75	Första utkastet	15.1.2021 KR, JK
0.90	Utkastsversion för kommentarer	3.5.2021 KR, JK
1.00	Publicerad version	19.5.2021 KR, JK

Innehållsförteckning

TTTT-modellen för säkert arbete

1 Inledning

Detta stödmaterial har utarbetats för organisationer inom den offentliga förvaltningen för att möjliggöra säkert arbete med tanke på den information som behandlas, de arbetsutrymmen som används och de verktyg som utnyttjas. Stödmaterialet grundar sig på god praxis inom riskhantering, kontinuitet, datasäkerhet och dataskydd som har sammanställts av experter från ledningsgruppen för digital säkerhet inom den offentliga förvaltningen (VAHTI). Genom att följa god praxis främjar vi samtidigt cybersäkerheten. Vi har som en del av utbildningarna i det digitala livet publicerat en cirka sex minuter lång utbildningsvideo som presenterar TTTT-modellen. Videon finns fritt tillgänglig:

TTTT-modellen - video

Den föregående videon publicerades som en del av webbutbildningen digital säkerhet för kommunernas förtroendevalda. Trots namnet innehåller utbildningen god praxis för oss alla

- utbildningens startsida

Likaså kommer vi att publicera andra kortare utbildningsvideor som främjar detta stödmaterial.

Vi hoppas att du ger oss respons på detta material. Efter att vi fått tillräckligt med förbättringar och korrigeringsförslag publicerar vi en uppdaterad version av detta.
Länk till responsenkäten.

Varför har säkert arbete blivit allt viktigare?

Betydelsen av säkert arbete har betonats under de senaste åren. Följande fyra observationer kan lyftas fram:

1) Utnyttjandet av digitala tjänster har blivit vanligare

    - Vi producerar allt fler tjänster i den digitala verksamhetsmiljön och använder dem allt mer själva, även på fritiden.

2) Coronaviruspandemin har påverkat vårt sätt att arbeta i den digitala världen

    - Coronaviruspandemin har förändrat vårt sätt att arbeta snabbare än någon annan tidigare förändring; i synnerhet har det skett en enorm ökning av antalet användare inom distansarbete. Vissa förändringar kommer att

vara bestående, även efter coronan, till exempel när det gäller distansarbete och nya tjänster och verksamhetsmodeller som tagits i bruk.

- Coronaviruspandemin utnyttjas aktivt i bedrägerikampanjer som genomförs av nätbrottslingar samt i andra attacker. Även i övrigt har aktiviteten bland nätbrottslingar och statliga aktörer ökat betydligt under det senaste året. Vi användare och de ICT-tjänster som vi använder attackeras med ständigt utvecklade och även med nya attacker. Till exempel får vi nu bedrägeri- och fiskemeddelanden och företag per telefon (bedrägerisamtal), textmeddelanden, e-postmeddelanden, snabbmeddelanden, försök till bedrägeri på webbplatser samt som företag som kommer via plattformar i sociala medier.

3) Betydelsen av behandling av personuppgifter och datasäkerhet har ökat

   - EU:s allmänna dataskyddsförordning, som blev tillämplig den 25 maj 2018, har ökat betydelsen av att behandla personuppgifter enligt kraven och genomföra informationssäkerheten. Var och en av oss vill vara säker på att våra personuppgifter behandlas på ett säkert och tillförlitligt sätt och vi måste även själva sörja för detta för vår del när vi sköter våra arbetsuppgifter.

4) Störningar i ICT-tjänsterna, personuppgiftsincidenter och cyberattacker har blivit vanligare

   - De största hoten mot vår digitala verksamhet är tekniska störningar i ICT-verksamheten, mänskliga misstag som vi själva har begått och nätbrottslingar. Beklagansvärt många problem i den digitala världen beror på oss själva. Särskilt i brådska ökar sannolikheten för fel. Tyvärr utvecklar nätbrottslingar sina metoder snabbare än vi kan utveckla våra skyddsmetoder.

Vi kan alla påverka de två sistnämnda punkterna. I detta stödmaterial beskriver vi sådan god praxis som undviker mänskliga misstag och försvårar nätbrottslingarnas verksamhet om vi följer den på ett ansvarsfullt sätt och enligt kraven.

God praxis som presenteras här är exempel som varje organisation kan använda som modell för att producera eller uppdatera sina egna anvisningar.

2 TTTT-verksamhetsmodellen möjliggör säker verksamhet

Detta stödmaterial baserar sig på verksamhetsmodellen TTTT. Den betyder

Identifiera och klassificera informationen

1) För att vi ska kunna agera säkert och hantera uppgifterna i enlighet med de krav som ställs på dem måste du identifiera vilken kategori av information du behandlar. Detta avgör i vilka lokaler och med vilka tjänster dessa uppgifter kan behandlas.

Identifiera platsen

2) När du har definierat klassificeringen av de uppgifter du behandlar ska du identifiera i vilka fysiska (arbets)lokaler dessa uppgifter kan behandlas.

Identifiera verktygen

3) När du har identifierat klassificeringen av de uppgifter du behandlar ska du veta med vilka apparater och hurdana digitala verksamhetsmiljöer, organisationens egna eller externa ICT-tjänster dessa uppgifter kan behandlas.

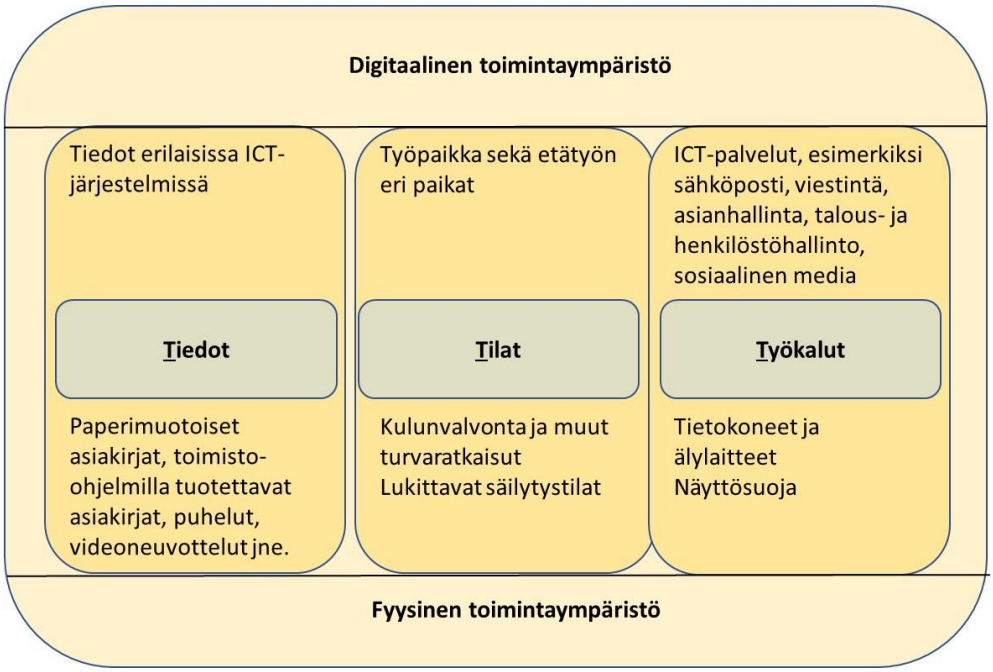

Bild 1. Med hjälp av TTTT-modellen kan du säkerställa att du hanterar uppgifterna säkert, enligt kraven och beaktar särdragen i den digitala och fysiska verksamhetsmiljön.

Förutom TTTT-modellen ska du innan du gör något **kontrollera och stanna upp** för att säkerställa att allt ser rätt ut. Kontrollera till exempel innan du skickar din e-post:

1) att e-posten har rätt mottagare

2) att meddelandet har rätt bilaga

3) att meddelandet skickas på rätt sätt, till exempel med krypterad e-post om den skickas utanför organisationen och innehåller personuppgifter eller sekretessbelagda uppgifter

4) och till exempel när du använder sociala medier, om bilden i uppdateringen av sociala medier är rätt och att den inte avslöjar uppgifter som inte hör dit, och om rätt personer har kopplats ("taggats") till uppdateringen

2.1 Riskhantering är grunden för allt säkert arbete

Alla ovan nämnda synvinklar förutsätter också identifiering av **hot och riskhantering**. När det gäller identifiering och klassificering av uppgifter ska man inte ta risker, utan i situationer där du inte är säker på hur uppgifterna klassificeras är det din skyldighet att utreda saken och vid behov be om hjälp. I användningen av lokalerna måste du alltid från fall till fall bedöma hur varje plats lämpar sig för behandling av de

uppgifter som behandlas. På motsvarande sätt får verktygen endast användas för behandling av sådan information som verktygen i fråga är avsedda för. Du får till exempel inte skicka sekretessbelagda handlingar eller personuppgifter utanför din organisation, om du inte har skyddat uppgifterna på något annat sätt, till exempel med krypterad e-post eller på något annat ändamålsenligt sätt. Se också till att sekretessbelagda uppgifter inte heller hamnar på någon oskyddad tjänst.

Riskhanteringen grundar sig på en bedömning av sannolikheten för att risken realiseras och dess konsekvenser. Ju större sannolikhet och riskens inverkan på verksamheten om den realiseras, desto större effekt har den åtgärd som du beslutar om när risken realiseras. När du lämnar jobbet, eller hemmet, tänker du på om du låste dörren. Det gjorde du nog, men hurdan risk uppstår det om dörren till exempel blev öppen under veckoslutet? De flesta går och kollar en extra gång - och genomför samtidigt riskhantering. Även om du inte själv märker det fattar du varje dag ett stort antal olika beslut, både på arbetsplatsen och i vardagen. Men i hur många av dem har man verkligen bedömt riskerna och effekterna?

Alla ska rapportera hot eller risker som observerats i arbetsuppgifterna och anmäla dem enligt organisationens anvisningar. Att sörja för säkerheten är allas vår sak.

3 Identifiera uppgifterna

Det är viktigt att de uppgifter du behandlar identifieras och klassificeras på rätt sätt, eftersom de två sista delområdena i TTTT-modellen grundar sig på att klassificeringen har skett på rätt sätt. Om du klassificerar uppgifterna fel kan det leda till otrygg behandling av uppgifterna. Uppgifterna kan hamna i händerna på aktörer som inte har rätt till dem. Eller en felaktigt klassificerad uppgift kan kräva fler åtgärder, till exempel om offentlig information behandlas felaktigt som sekretessbelagd och därmed förhindrar att informationen utnyttjas.

I allmänhet klassificeras uppgifterna enligt personuppgifterna och deras sekretess. Ingår någondera i uppgifterna? Finns det något annat speciellt med dem? Gäller klassificeringen hela dokumentet eller bara en del av det? I alla fall ska man hålla fast vid informationens integritet och tillgänglighet i enlighet med kraven på korrekt klassificering.

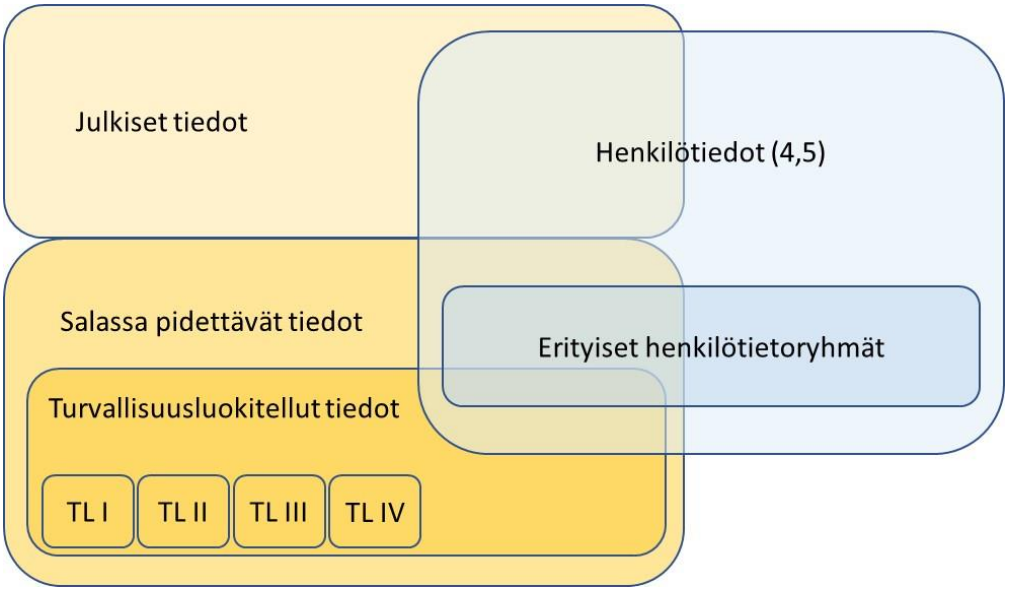

Bild 2. Exempel på olika nivåer i klassificeringen av uppgifter. Observera att personuppgifter också kan vara offentliga, men vanligtvis är de sekretessbelagda.

Bild 3. Exempel på olika nivåer i klassificeringen av uppgifternas offentlighet. Obs, säkerhetsklassificerade uppgifter kan endast klassificeras inom statsförvaltningen och för dem används nivåerna I, II, III och IV. Av dessa behöver I och II särskilda lokaler för behandlingen och det finns särskilda krav på överföringen av uppgifterna.

3.1 Personuppgifter

Var och en av oss ska kunna identifiera vilka uppgifter som är personuppgifter och vilka av dem som hör till särskilda kategorier av personuppgifter. En omfattande anvisning finns på Dataombudsmannens byrås webbplats (https://tietosuoja.fi/sv/vad-ar-en-personuppgift)

"Personuppgifter är alla uppgifter som anknyter till en identifierad eller identifierbar person. Med andra ord är personuppgifter sådana uppgifter utifrån vilka en person kan identifieras direkt eller indirekt till exempel genom att kombinera en enskild uppgift med en annan uppgift, som möjliggör identifiering. En person kan identifieras till exempel utifrån namn, personbeteckning eller en omständighet som är karakteristisk för honom eller henne. ”

Vi rekommenderar att alla anställda inom den offentliga förvaltningen och andra organisationer genomför webbutbildningen:
Dataskyddets ABC för anställda inom offentlig förvaltning 2020

3.2 Särskilda kategorier av personuppgifter

Var och en av oss ska också identifiera vilka uppgifter som hör till särskilda kategorier av personuppgifter. Anvisningar om dessa finns i Dataombudsmannens byrås anvisning (https://tietosuoja.fi/sv/behandling-av-sarskilda-kategorier-av-personuppgifter):

Av dessa uppgifter framgår personens

1) ras eller etniska ursprung
2) politiska åsikter
3) religiösa eller filosofiska övertygelse
4) medlemskap i fackförbund
5) hälsouppgifter
6) sexuella läggning eller sexuella beteende
7) genetiska och biometriska information för identifiering av en person.

Dessa uppgifter måste skyddas särskilt noggrant, eftersom behandlingen av dem kan medföra betydande risker för en persons grundläggande rättigheter och friheter.

De uppgifter som hör till dessa kategorier behandlas vanligtvis kvantitativt mest i organisationer inom den offentliga förvaltningen. Dessutom behandlar många av oss dem på fritiden till exempel i anslutning till den egna eller de närståendes hälsovård.

Särskild uppmärksamhet bör fästas vid behandlingen av hälsouppgifter, eftersom nätbrottslingar har upptäckt deras höga marknadsvärde. För att få tag i dem utvecklar de nya attacker mot informationssystem och användare.

Kom ihåg! När personuppgifter efterfrågas, kontrollera alltid vem som frågar, varför och för vilket ändamål - lämna inte ut uppgifterna förrän du är säker på att det till exempel inte är fråga om ett bedrägeriförsök. Var särskilt försiktig med frågor som kommer från e-post, sms, snabbmeddelanden eller webbsidor.

3.3 Offentliga handlingar

All information är offentlig om den inte är sekretessbelagd enligt lag. Personuppgifter kan också vara offentliga, men även i det fallet får de endast behandlas inom ramen för dataskyddslagstiftningen.

Datasäkerhet förutsätts också i behandlingen av offentlig information. Datasäkerheten omfattar åtgärder för att garantera informationens tillgänglighet, integritet och konfidentialitet. Även om offentlig information inte förutsätter sekretess, dvs. konfidentialitet, ska man dock alltid se till att de två andra delområdena i informationssäkerheten, dvs. integriteten och tillgängligheten, genomförs.

Även om det i Finland inte finns särskilda krav på informationens integritet och tillgänglighet kan de definieras genom att man klassificerar datasystemen utifrån den funktionella betydelsen av de uppgifter de innehåller och hur kritiska uppgifterna är. Till exempel är en webbtjänst som publicerar en offentlig lunchmeny för organisationens personalmatsal inte lika kritisk med tanke på informationens integritet eller tillgången till tjänsten som en tjänst som innehåller de anvisningar och kontaktuppgifter som behövs vid störningar i organisationens verksamhet.

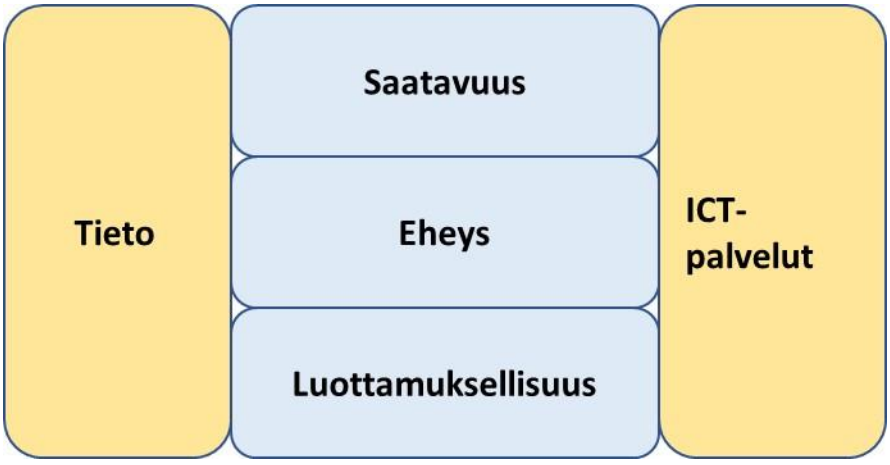

Bild 4. Med hjälp av informationssäkerheten sörjer man för tillgången, integriteten och konfidentialiteten i fråga om information och tillhörande ICT-tjänster och utrustning.

3.4 Sekretessbelagda handlingar

Bestämmelser om anteckningar om sekretess i handlingar finns i 25 § i lagen om offentlighet i myndigheternas verksamhet (https://www.finlex.fi/sv/laki/ajantasa/1999/19990621). Varje organisation inom den offentliga förvaltningen ska ha anvisningar och utbildning om hur denna klassificering genomförs.

3.5 Säkerhetsklassificerade handlingar

Bestämmelser om säkerhetsklassificerade handlingar finns i 18 § i lagen om informationshantering inom den offentliga förvaltningen (https://www.finlex.fi/sv/laki/alkup/2019/20190906) och lyder som följer:

”Myndigheter vid statliga ämbetsverk och inrättningar, domstolar och nämnder som har inrättats för att behandla besvärsärenden ska säkerhetsklassificera handlingar och förse dem med anteckning om säkerhetsklass som visar vilket slag av informationssäkerhetsåtgärder som ska vidtas vid behandlingen av dem. Anteckning om säkerhetsklass ska göras, om en handling eller informationen i den är sekretessbelagd enligt 24 § 1 mom. 2, 5 eller 7–11 punkten i lagen om offentlighet i myndigheternas verksamhet och om obehörigt avslöjande eller obehörig användning av handlingen kan orsaka skada för försvaret, för förberedelser inför undantagsförhållanden, för internationella relationer, för brottsbekämpningen, för den allmänna säkerheten eller för stats- och samhällsekonomins funktion, eller på något annat jämförbart sätt för Finlands säkerhet.”

Närmare krav på behandlingen av säkerhetsklassificerad information utfärdas i statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen. https://www.finlex.fi/sv/laki/alkup/2019/20191101

Informationshanteringsnämnden har publicerat en rekommendation om detta 18.1.2021: http://urn.fi/URN:ISBN:978-952-367-500-1

4 Identifiera platsen

När du har identifierat klassificeringen av de uppgifter du behandlar påverkar det direkt i vilka lokaler uppgifterna kan behandlas. I detta stödmaterial beskrivs lokalernas inverkan på behandlingen av uppgifter på en allmän nivå. Varje organisation ska själv fastställa närmare anvisningar som personalen ska följa.

Även om vår verksamhet i allt högre grad har övergått till en digital verksamhetsmiljö är vi ändå alltid närvarande i någon fysisk verksamhetsmiljö.

t

Bild 5. Behandlingen av informationen sker säkrast i de arbetsutrymmen som arbetsgivaren erbjuder. Om statsförvaltningens organisation behandlar säkerhetsklassificerade uppgifter ska separata anvisningar ges om behandlingen av och utrymmena för detta.

4.1 Arbetsplats

Din arbetsgivare har skapat säkra arbetsutrymmen i de lokaler som står till ditt förfogande. Förutom fysiska säkerhetskonstruktioner (väggar, portar, passagekontroll, lås, larmanordningar och övervakningsanordningar) skyddas du av säkra datakommunikationsförbindelser och säkerhetslösningar. Beroende på klassificeringen av de uppgifter du behandlar och organisationens anvisningar kan det vara möjligt att behandla en del av uppgifterna endast i arbetsgivarens lokaler. Då är det inte tillåtet att behandla dem någon annanstans, såsom i distansarbete hemma, under en arbetsresa, i en annan organisations lokaler eller i offentliga lokaler.

4.2 Arbetsplatsens säkerhetsklassificerade utrymmen

Statsförvaltningens organisationer ska ge anvisningar om i vilka lokaler säkerhetsklassificerade uppgifter kan behandlas. Enligt 9 § i förordningen om säkerhetsklassificering ska informationshanteringsenheten definiera fysiskt skyddade säkerhetsområden för att skydda behandlingen av säkerhetsklassificerade handlingar och informationssystemen. Säkerhetsområdena är administrativa områden och skyddsområden. Information om dessa finns i Informationshanteringsnämndens rekommendation ”Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä” i kapitlet ”Asiakirjan käsittelyn ja tietojärjestelmien suojaaminen turvallisuusalueiden avulla”.

4.3 Distansarbete

Distansarbetets betydelse har ökat i och med de möjligheter som den nya teknologin erbjuder; arbete oberoende av tid och plats kommer att bli allt vanligare på 2020-talet. På motsvarande sätt kan vi i allt högre grad sköta ärenden som gäller fritiden med hjälp av digitala tjänster.

Traditionellt uppfattas distansarbete som arbete som utförs hemma. Med distansarbete avses dock allt arbete som utförs utanför arbetsplatsen, vare sig det sker hemma, på sommarstugan, på en arbetsresa i hemlandet eller utomlands, på ett café eller i kundens eller samarbetspartnerns lokaler.

Vid distansarbete ska man beakta följande på en allmän nivå, varje organisation preciserar vanligtvis dessa anvisningar:

a) Hantering av informationsmaterial i pappersformat

- säkerställ att informationsmaterialet transporteras på ett säkert sätt från arbetsplatsen till distansarbetsplatsen enligt de anvisningar du har fått
- säkerställ att informationsmaterialet inte i något skede hamnar i utomståendes händer
- säkerställ att både offentliga och i synnerhet personuppgifter och eventuella sekretessbelagda uppgifter förvaras i låsta utrymmen
- se till att uppgifterna förstörs på ett säkert sätt enligt organisationens anvisningar, förstör inte uppgifterna själv hemma utan följ processen
- säkerställ att informationsmaterialet returneras till arbetsplatsen i det skede då det är möjligt

b) Säker användning av ICT-utrustning och tjänster

- se till att datorns skärm är placerad så att utomstående personer inte ser den inifrån eller utifrån
- säkerställ att dataskyddsfilter (s.k. privacy filter) används på bärbara datorer och

på sådana skärmar där det finns risk för att utomstående kan se uppgifterna. Det lönar sig också att fästa uppmärksamhet vid skärmens ljusstyrka, eftersom en för klar skärm kan tömma användningen av dataskyddsfiltret. Observera att även om filtret är i bruk kan uppgifterna ändå vara synliga direkt bakifrån.

- Ha alltid arbetsgivarens utrustning med dig och lämna den inte på en obevakad plats.

- Stäng av datorn i slutet av arbetsdagen. På så sätt försvårar du en eventuell tjuvs åtkomst till informationen på arbetsstationen, särskilt när hårddisken på arbetsstationen är krypterad.

c) Samtal

- När du talar i telefon eller deltar i webbmöten ska du beakta andra personer i samma rum och anpassa det samtal som förs till situationen. Om det finns andra personer på plats, använd hörlurar istället för apparatens egen eller externa högtalare. Observera att ljudet också kan spridas utanför lokalen.

- om du har t.ex. en smarthögtalare hemma ska du stänga av den när du sköter dina arbetsuppgifter.

d) Personligt ID

- Förvara de passernycklar och identitetskort som arbetsgivaren gett dig på ett säkert sätt.

- Ha alltid identitetskortet synligt när du rör dig på din arbetsplats för att man ska veta vem som har rätt att vistas i lokalerna. Utomstående personer utan kort ska på de flesta ställen anmäla sig i receptionen och de får ett eget besöksnummer. Anmäl obekanta personer som inte kan uppvisa ett lämpligt identitetskort och släpp inte in okända personer då du öppnar dörren!

e) Val av nätverk (internetanslutning)

När du arbetar utanför arbetsplatsen eller distansarbetsplatsen hemma ska du vara noggrann med den internetanslutning som används. I allmänhet erbjuder din arbetsgivare en VPN-förbindelse som krypterar datakommunikationsförbindelsen antingen till arbetsgivarens nätverk eller till VPN-leverantörens server. Det försvårar nätbrottslingarnas attacker och krypterar information som går via datakommunikationsförbindelsen. Bärbara datorer använder ofta trådlöst nätverk (WLAN/WIFI). Det är viktigt att

identifiera om trådlöst nätverk är öppet eller skyddat. Ett skyddat trådlöst nätverk identifieras i allmänhet av en låsbild bredvid nätverkets symbol. Det innebär att det behövs ett lösenord för att använda nätet. Om du använder ett öppet trådlöst nätverk utan VPN-anslutning är du utsatt för olika attacker av nätbrottslingar. Ett säkrare sätt än det öppna nätet är att dela internetförbindelsen från din egen smarttelefon. Då går datakommunikationsförbindelsen direkt till datakommunikationsoperatörens nät utan oidentifierade apparater emellan. Användningen av telefonen som basstation kräver mycket av batteriet så det lönar sig att hålla enheten i laddning.

4.3.1 Distansarbete hemma

För distansarbete behövs en internetanslutning, som kräver en "nätadapter", till exempel en router, usb-modem eller adsl/vdsl/kabel/fibermodem. Även en smarttelefon kan fungera som en nätverksenhet genom att dela internetförbindelsen med andra enheter.

För att trygga säkerheten i hemnätet räcker det ofta med ett lösenord för apparaten och det nätverk den bildar. Dessutom ska det säkerställas att nätverksenheten har uppdaterats till den senaste programversionen eller att automatiska uppdateringar används. Dessutom måste standardlösenorden som gör det möjligt att hantera apparaten bytas ut. Anvisningar för kontroll av dessa finns i bruksanvisningen som följer med nätapparaten. Om nätverksenhetens informationssäkerhet inte har säkerställts kan nätbrottslingar använda sårbara apparater till exempel för att kapa nättrafiken eller genomföra överbelastningsattacker. Beakta också den praxis som lyfts fram i föregående kapitel gällande valet av internetanslutning.

4.3.2 Distansarbete i offentliga lokaler

I offentliga lokaler är det endast tillåtet att behandla offentliga uppgifter om din organisation inte har gett andra anvisningar om detta. Utöver ICT-tjänsterna ska detta också beaktas i hanteringen av material i pappersform samt i diskussioner till exempel per telefon eller på webbmöten. I offentliga lokaler ska man vara noggrann också så att ingen utomstående kan kunna påverka tillgången till eller integriteten hos den offentliga information som behandlas. Här ingår såväl åtkomst till apparaten genom skenmanöver som att ta den med våld. Det lönar sig att identifiera sådana offentliga uppgifter vars förlust eller ändring av integritet, såsom förfalskning, kan medföra en klar risk för dig eller din organisation.

Eftersom detta stödmaterial grundar sig på god praxis kan organisationerna till exempel i fråga om detta - liksom de övriga punkterna i detta stödmaterial - ha egna tillämpningsanvisningar där säkerheten förbättras genom vissa tilläggsåtgärder.

4.3.3 Distansarbete under arbetsresa i hemlandet

Under arbetsresor i hemlandet ska man framför allt se till att informationsmaterial och ICT-apparater som används är säkra. Du ska hela tiden hålla uppsikt över dem under resan och de ska till exempel inte placeras i lastrummet i flygplan eller bussar.

Om du under din resa får till exempel affärspresenter som kan kopplas till din arbetsstations USB-port eller trådlösa WLAN/WiFi, kan de användas för att sprida skadliga program eller samla in information. Därför lönar det sig inte att ansluta USB-minnen, apparater som ansluts till internet, reservströmbanker eller fläktar till din arbetsstation, arbetstelefon eller ditt trådlösa nätverk.

4.3.4 Distansarbete på arbetsresa utomlands och utomlands

Vid arbete utomlands ska man beakta samma hot och anvisningar som vid arbete i Finland. Dessutom ska även andra säkerhetsrelaterade omständigheter beaktas. Du får mer information om hanteringen av datamaterial eller användningen av terminaler utomlands i din organisations egna anvisningar.

En god praxis är att en person som reser utomlands får tillgång till en dator och smarttelefon som endast är avsedd för resor. Alla onödiga funktioner har gallrats bort från enheterna och man har även i övrigt strävat efter att stärka deras säkerhet. När du återvänder från resan returnerar du enheterna och de ominstalleras före nästa användning. På så sätt minskar man också den risk som uppstår om någon lyckas bryta datasäkerheten i enheterna under resan. Anslut alltså inte resedatorn direkt efter att du har återvänt till nätverket på din arbetsplats, så att inget tar sig förbi nätverkets skydd.

Om du deltar i ett internationellt webbseminarium eller motsvarande evenemang (även från Finland på distans) ska du vara särskilt försiktig om du efter ett sådant evenemang får nätverksbegäran eller andra kontakter via sociala medier. Deltagarlistorna för sådana evenemang är ofta offentliga och erbjuder missbrukare ett enkelt sätt att närma sig dig och försöka komma in i dina nätverk.

När du rör dig utomlands lönar det sig också att använda sociala medier måttligt. Till exempel information om var du befinner dig och vart du är på väg samt syftet med din resa kan vara användbar information för nätbrottslingar eller andra missbrukare.

När man rör sig utomlands lönar det sig alltid att använda VPN-förbindelse, om det är möjligt att använda en sådan i landet. Om du tänker använda mobiltelefonförbindelsen utomlands, särskilt utanför EU-området, lönar det sig att först bekanta sig med prislistan för den operatör som arbetsgivaren anlitar. I många länder ingår inte dataöverföring i anslutningens grundavgift, så försök undvika överraskande telefonräkningar till arbetsgivaren.

Organisationen kan utnyttja nedanstående VAHTI-anvisning vid utarbetandet av sina anvisningar för utlandet:

VAHTI 4/2013 Stödmaterial för personalens datasäkerhetsanvisning - bilaga 9 avsnitt 6 om beaktandet av datasäkerheten vid resor till eller arbete utomlands.

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

VAHTI- sekretariatet

3.5.2021

5 Identifiera tillgängliga apparater och verktyg

TTTT-modellens sista delområde gäller tillgängliga verktyg, alltså apparater och tjänster. I praktiken bestämmer klassificeringen av informationsmaterial direkt hurdana apparater och tjänster som kan användas vid behandlingen av dem. Avvik inte från organisationens anvisningar.

Du kan tillämpa den praxis som beskrivs här vid inte bara på dina arbetsuppgifter utan även på apparater och tjänster som används på fritiden.

5.1 ICT-utrustning som arbetsgivaren tillhandahåller

5.1.1 Datorer

Terminaler som är avsedda för personalen, såsom datorer och smarttelefoner, är endast avsedda för den egna personalen. De får inte användas av utomstående, inte ens av familjemedlemmar.

Utgångspunkten är alltså att arbetsuppgifterna alltid ska utföras med apparater som arbetsgivaren ställer till ditt förfogande. Om din arbetsgivare tillåter är det möjligt att behandla offentlig information med andra enheter än arbetsgivarens. Behandling av annan än offentlig information med en enhet i personligt ägo kan inte anses rekommenderat eftersom informationen via enheterna kan hamna på en oönskad plats utan att man märker det. Till exempel kan säkerhetskopieringstjänster som finns i molnet hos vissa utrustningstillverkare eller andra tjänster som används på din fritidsenhet ligga utanför EU-området. Då får personuppgifter som hänför sig till arbetsuppgifterna inte hamna i tjänsterna på ett okontrollerat sätt. Representanter för utländska underrättelsetjänster kan också få tillgång till dessa tjänster enligt den nationella lagstiftningen. Därför ska sekretessbelagda uppgifter inte behandlas med en enheter i din personliga ägo.

Det är viktigt att alla terminaler har ett lösenord, en pinkod eller en biometrisk identifikation för att öppna enheten. Terminalerna ska också låsas automatiskt när arbetet med dem upphör. På så sätt hålls apparaterna låsta när de inte används.

För terminalernas del ska man också se till att operativsystemen och programmen är uppdaterade. Ofta installeras uppdateringarna centraliserat på arbetsgivarens enheter, och användaren ansvarar då för att de automatiska uppdateringar som terminalen föreslår utförs. Vid behov ska apparaten startas om för att slutföra uppdateringarna så snart som möjligt. Se också till att uppdatera de enheter du använder på fritiden.

5.1.2 Mobila enheter

För många är det en automatisk handling att sörja för datorns informationssäkerhet. Det är också lika viktigt att sörja för datasäkerheten i en telefon eller smart enhet, eftersom telefonen ofta har tillgång till samma information och tjänster, såsom e-post och kalender. En telefon som smittats av skadlig programvara fungerar också som ett bra hjälpmedel för brottslingar för att lokalisera offrets placering, avlyssna offret eller fotografera i hemlighet.

Du kan förbättra din telefons eller smarta enhets informationssäkerhet med några enkla åtgärder:

1. Läs användarvillkoren för applikationerna

Godkände du användarvillkoren då du installerade en ny applikation utan att läsa dem? I användarvillkoren eller i den dataskyddsbeskrivning som finns tillgänglig finns information om vilka personuppgifter applikationen samlar, för vilket ändamål de används och till vilka instanser de förmedlas. Dessutom berättar de om användarens rätt till sina personuppgifter samt hur länge personuppgifterna förvaras till exempel efter att kontot har tagits bort.

2. Uppdatera enhetens programvara

På datorn eller telefonen är operativsystemet apparatens hjärna, som repareras och förbättras genom uppdateringar. Uppdateringarna kan reparera fel i en tidigare version eller lägga till nya funktioner. Det är rekommenderat att uppdatera operativsystemet eftersom det kan finnas fel i ett föråldrat program. De kan innehålla sårbarheter som gör det möjligt att ta kontroll över en smarttelefon med hjälp av ett skadligt program. Dessutom rekommenderas att man aktiverar den egenskap med vilken en smarttelefon automatiskt uppdaterar operativsystemet.

3. Uppdatera applikationerna

Förutom operativsystemet måste även de applikationer som installerats i smarttelefonen uppdateras. Deras programfel kan i värsta fall ge utomstående åtkomst till applikationens (eller telefonens) uppgifter. I telefonens inställningar kan man välja att telefonen automatiskt uppdaterar applikationerna.

4. Kontrollera applikationernas rättigheter

Då en ny applikation tas i bruk frågar den vilka av telefonens funktioner den kan använda eller vilken information den har tillgång till, till exempel fotografier och filer. Här lönar det sig att vara noggrann och endast ge applikationen de rättigheter som är nödvändiga för dess användningsändamål. En navigeringsapplikation behöver inte ges behörighet att använda telefonens bilder och ett bildbehandlingsprogram behöver inte använda telefonens mikrofon. Applikationernas rättigheter kan ändras i telefonens inställningar.

Om appen vill använda enhetens kamera eller mikrofon och det inte finns någon tydlig grund, lönar det sig att förhindra användningen efter att applikationen har installerats.

5. Var noggrann med enheter som använder USB-anslutning

Via datorns USB-port överförs förutom ström även data till den mobila enheten, så via den kan skadliga program spridas.

En bra allmän regel är att du tillsammans med arbetsgivarens utrustning endast använder de USB-apparater som arbetsgivaren erbjuder. Kom ihåg detta särskilt med

minnesstickor, eftersom skadliga program kan överföras till arbetsgivarens arbetsstation via stickor som är i personligt bruk.

5.2 Tjänster som arbetsgivaren tillhandahåller

Din arbetsgivare erbjuder ICT-tjänster för att du ska kunna sköta ditt arbete. Det är din skyldighet att använda dem enligt givna anvisningar.

5.2.1 Inloggning i tjänsterna

Inloggningen i tjänsterna är ett av de mest kritiska skedena i användningen av en digital tjänst med tanke på säkerheten. Nedan presenteras de vanligaste sätten att logga in på tjänsterna och god praxis i anslutning till dem.

När webbtjänster används framhävs betydelsen av ett bra lösenord, eftersom samma användarnamn kan användas för att hantera flera tjänster. Facebook-, Apple-, Google- eller Office 365-konton kan användas för att logga in på flera olika tjänster, till exempel kalender, lagringsutrymme och e-post, och eventuellt även tredjepartstjänster. Om lösenordet hamnar i fel händer får utomstående tillgång till alla dessa tjänster och de uppgifter som sparats i dem. Man ska inte identifiera sig i tjänster med anknytning till arbetsuppgifterna med hjälp av ovan nämnda tjänster i sociala medier, utan logga in i varje tjänst med en e-postadress i arbetet eller med någon annan identifieringsmetod som arbetsgivaren erbjuder.

Du ska vara särskilt noggrann med lösenordet till e-posttjänsten, eftersom du loggar in i flera tjänster med hjälp av e-postadressen som användarnamn. Det går att byta lösenordet för många tjänster med hjälp av e-postadressen, så om e-postkontot är i fel händer går det också komma åt andra tjänster.

5.2.2 Säker hantering av lösenord

I den digitala världen motsvarar lösenordet nycklarna i den fysiska världen. Den får inte hamna i fel händer. Man ger inte nycklarna till utomstående, och samma noggrannhet och försiktighet ska iakttas med lösenord.

Ett bra lösenord ska vara:

1. **Minneslista**

Ett av lösenordets viktigaste egenskaper är att det går att komma ihåg. Om lösenordet inte går att komma ihåg är det lät hänt att det blir nedskrivet. Då kan det hamna i händerna på utomstående. Om du skriver lösenordet på papper eller sparar det på en dator eller smart enhet ska du spara det så att det inte direkt framgår av lösenordet till vilken tjänst det är avsett samt vid behov lägga till tilläggstecken efter eller i början av lösenordet för att förhindra missbruk.

2. **Långt**

Enligt nuvarande uppgifter är lösenordets längd viktigare än dess komplexitet, dvs. till exempel antalet specialtecken som ingår i lösenordet. När datorernas beräkningseffekt växer ökar också nätbrottslingarnas möjligheter att ta reda på lösenordet för tjänsterna med hjälp av lösenord som erhållits med hjälp av dataintrång. Då längden ökar tar det även mer tid att bryta lösenordet. Ett bra sätt är att skapa en lösenordsmening istället för ett lösenord. Meningen kan även göras svårare att gissa genom att använda dialektord eller byta ut bokstäver mot siffror. Men se även då till att lösenordet lätt går att minnas.

3. Unikt

Nätbrottslingar samlar in och publicerar lösenord och användarnamn för de inbrott som görs och försöker med hjälp av dem bryta sig in i andra tjänster. Därför ska samma lösenord inte användas i olika tjänster.

Du kan söka inspiration för att hitta på goda lösenord på Traficoms kampanjwebbplats Ju längre desto bättre på adressen: https://pidempiparempi.fi/

Biometrisk identifikation

Med biometrisk identifiering avses identifiering som baserar sig på människans fysiologi. Som identifikation kan man använda till exempel fingeravtryck eller en ansiktsbild. Den utrustning som används för detta varierar fortfarande och den här typen av identifikation bör inte vara det enda skyddet. Det fingeravtryck som ges för en privat enhet ska inte heller användas i arbetsutrustningen.

Två- eller annan multifaktorsautentisering

I en del tjänster som arbetsgivaren erbjuder eller som används på fritiden är det möjligt att använda identifiering i två eller flera skeden. Då säkerställer tjänsten användarens identitet i två skeden. I första steget efterfrågas tjänstens fasta lösenord och det andra steget kan vara att mata in en nummerserie som skickats till mobiltelefonen eller en begäran om godkännande i en separat applikation. En identifiering i två steg säkerställer att utomstående inte kan använda tjänsten även om de har fått tjänstens lösenord. Om det är möjligt att använda tvåfaktorsautentisering i tjänsten rekommenderas detta.

Program för hantering av lösenord

Programmet för hantering av lösenord är en applikation där olika tjänsters lösenord kan sparas. Det möjliggör unika lösenord av hög kvalitet. Programmet ser automatiskt till att lösenordet matas in när en webbtjänst frågar efter det. Programmets fördel är att användaren bara behöver komma ihåg ett lösenord – programmet minns resten. Risken är att om lösenordet hamnar i fel händer hamnar även de lösenord som sparats i lösenordet. Om din arbetsgivare erbjuder ett program för hantering av lösenord rekommenderas det. Då ska du vara särskilt noggrann med lösenordet i detta hanteringsprogram, som ligger bakom alla andra lösenord.

5.2.3 E-post och krypterad e-post

I de flesta organisationer kan man internt behandla sekretessbelagda uppgifter som innehåller personuppgifter per e-post när e-post inte försvinner till en adress utanför organisationen (dvs. hålls kvar på servern). Bekanta dig med din organisations anvisningar.

Dessutom används ofta en krypterad e-posttjänst som gör det möjligt att skicka sekretessbelagda uppgifter eller personuppgifter till mottagare utanför organisationen samt vid behov inom organisationen, om organisationens anvisningar förutsätter det.

När e-post skickas ska man fästa uppmärksamhet vid det fält där mottagarens e-postadress matas in. I allmänhet är alternativen mottagare (to), kopia (cc) och dold kopia (bcc). I vissa e-postprogram (till exempel Outlook) kan ett dolt kopieringsalternativ vara dolt. Om du använder fälten mottagare och kopia visas alla mottagares e-postadresser för alla mottagare. Detta ska beaktas särskilt när man skickar e-post med stor spridning eller när man svarar på ett sådant meddelande; var noggrann om du endast vill svara på meddelandet till avsändaren eller alla som fått det.

Då du använder fältet dold kopia ser det ut som om mottagaren är meddelandets enda mottagare, även om meddelandet har kunnat skickas till en stor grupp mottagare.

Ofta föreslår e-postprogrammen mottagaren automatiskt utifrån det du skrivit. Var noga med då du väljer bland de förslagna alternativen. I vissa program kan förslagen tas bort från listan genom att klicka på krysset vid namnet.

Det lönar sig att fästa uppmärksamhet vid avsändarens e-postadress, eftersom den är lätt att förfalska. Dessutom kan man lura användaren genom att skapa en e-postadress som innehåller extra tecken eller där en liten L-bokstav har ersatts med stor I-bokstav. Ju viktigare meddelandet är, desto viktigare är det att säkerställa att mottagarens adress säkert är korrekt och korrekt skriven.

Bilagor i e-postmeddelandet är ett sätt att sprida skadliga program. Var därför misstänksam mot alla bilagor som kommer från en okänd avsändare. Skadliga program kan innehålla bilagor till Microsoft Office-program som kräver att så kallade makron tillåts när de öppnas. Svara alltid nej på frågan om makron och kontakta din organisations ICT-stödtjänst.

Via e-post skickas bedrägerier och med hjälp av dem fiskar man också inloggningsuppgifter, såsom lösenord. Den falska e-postens avsändaruppgifter kan se exakt likadana ut som den ursprungliga e-postadressen. Länken i e-postmeddelandet, med hjälp av vilken man till exempel ber om granskning av de egna uppgifterna ska kontrolleras, innehåller dock ett avvikande tecken. Syftet är att styra mottagaren till en förfalskad webbplats som ser rätt ut och som ligger på en helt annan webbadress. Användarnamn och lösenord som matats in på denna webbplats hamnar i nätbrottslingens händer. Om länken i meddelandet är misstänkt lönar det sig att glömma den och granska de egna uppgifterna genom att logga in direkt på tjänsteleverantörens genuina sida.

5.2.4 Kalendern

Kalenderns innehåll är ofta tillgängligt för hela personalen i organisationen. Därför ska man inte bifoga sekretessbelagda eller personuppgifter eller filer som innehåller sådana till kalenderhändelserna. Av personuppgifterna får endast e-postadresserna till de personer som kallas till mötet fogas till kalenderanteckningen.

5.2.5 Snabbmeddelanden

Som standard ska snabbmeddelanden endast användas för att förmedla offentlig information. En del av snabbkommunikationsapplikationerna är begränsade till att användas endast på fritiden, varvid användningen av dem till exempel för att sköta arbetsuppgifter strider mot användarvillkoren. Ett möjligt användningssätt är att använda ett snabbmeddelande för att skicka en påminnelse om att mottagaren har fått ett viktigt e-postmeddelande. Då sker den egentliga kommunikationen i en säkrare verksamhetsmiljö. En del organisationer kan erbjuda personalen en sådan snabbmeddelandetjänst, till exempel Skype eller liknande, som också gör det möjligt att behandla sekretessbelagda uppgifter och personuppgifter.

5.2.6 Webbkonferenstjänster

Förutom snabbmeddelanden ska man även vid webbkonferenstjänster vara noggrann med vilka uppgifter som kan behandlas på mötet och vilka uppgifter som får sparas i tjänsten.

Se till att personuppgifter eller sekretessbelagda uppgifter inte finns till exempel i kamerans synfält, där de syns för andra på mötet.

5.2.7 Säkerhetskopiering

Det är särskilt viktigt att säkerhetskopiera uppgifterna på arbetsstationen. Det kan hjälpa om hårddisken går sönder eller om ett utpressningsprogram låser och krypterar informationen på arbetsstationen. Om arbetsstationen smittats med ett skadligt program kan datorn återställas till tidigare läge med hjälp av en säkerhetskopia. Ta reda på hur säkerhetskopieringen har genomförts i din organisation. Ibland säkerhetskopieras till exempel endast en viss mappstruktur på din dator. Se också till att säkerhetskopiera uppgifterna om smarta enheter på fritiden, till exempel för fotografier.

5.3 Sociala medier

Sociala medier har blivit ett verktyg som allt fler organisationer nästan i realtid kan använda för att följa aktuella händelser, nätverka, öka sin egen sakkunskap och kommunicera om arbetsuppgifter.

De sociala medierna erbjuder fantastiska möjligheter om de utnyttjas på rätt sätt, men på samma sätt finns det en del särskilda hot som måste beaktas.

- Användaren kan i misstag dela eller skicka sekretessbelagda uppgifter till tjänsten. Om tjänsten ligger utomlands eller upprätthålls av en tredje part kan det vara

omöjligt att radera materialet eller så tar det så länge att informationen hinner läcka och spridas även till andra webbtjänster, varvid datamaterialet blir kvar på nätet för alltid.

- Användaren kan omedvetet orsaka en dataläcka. Även om de enskilda meddelandena inte utgör ett hot, kan man genom att samla uppgifter om olika tjänster eller en längre tidsperiod skapa en helhetsbild som leder till att konfidentiell information avslöjas.

- Även en annan person kan oavsiktligt avslöja konfidentiella uppgifter om användaren eller organisationen i meddelanden, fotografier eller videofiler som personen skickat till tjänsten. Därför lönar det sig alltid att kontrollera alla meddelanden och meddelanden som du är kopplad till ("taggad i").

12 Kontrollista för säker användning av sociala medier:

1. Ta reda på och följ organisationens policy för användning av sociala medier, där det i allmänhet också finns anvisningar om informationssäkert beteende.

2. Var särskilt försiktig när du öppnar meddelanden till dig som varnar för informationssäkerhetsfrågor och som ber dig skydda dig mot olika hot genom att klicka på en länk i meddelandet. Var försiktig även om ett sådant meddelande kommer från en person som du litar på och känner väl. Kontakta personen i fråga till exempel per telefon eller annan kommunikationskanal och kontrollera att meddelandet är äkta. Du kan också söka mer information om varningen eller eventuella bedrägerier i anslutning till den på webben. Var även mycket misstänksam till alla meddelanden som är ”alldeles för billiga eller för bra för att vara sanna”. Det lönar sig att inte öppna dem och absolut inte klicka på länken.

3. Om du misstänker att du blivit lurad eller offer för en attack ska du inte tveka med att be om hjälp. Anmäl absolut saken enligt din organisations anvisningar. Låt heller inte bli att göra polisanmälningar på fritiden även om den ekonomiska förlusten för din del kan bli anspråkslös.

4. Om du nämner din arbetsgivare i din profil på de sociala medierna uppträder du då som organisationens representant. Även i övrigt, om du behandlar arbetsärenden i tjänsten är du representant för din organisation. Kom ihåg att uppföra dig! Om du representerar ditt företag på de sociala medierna kan du också bli föremål för långvariga utbrott mot företaget. Säkerställ förfaringssätten med din arbetsgivare på förhand vid behandlingen av dessa. Tips vid hatretorik finns bland annat på adressen: https://valtiolla.fi/tukimateriaali-auttaa-kasittelemaan-tyossa-kohdattavaa-vihapuhetta/

5. Var försiktig med att mata in för personlig eller detaljerad information, fotografier eller annat material om dig själv, dina närstående eller din organisation. Observera att tjänsteleverantören eller en annan person i ditt nätverk i stor utsträckning kan utnyttja de uppgifter som du matar in i din profil. Bekanta dig med avtalsvillkoren för de tjänster du använder.

6. Kontrollera inställningarna för användarprofilens integritetsskydd och ändra dem vid behov så att dina uppgifter inte sprider sig längre än till önskade användare. Du kan också försöka begränsa synligheten hos enskilda meddelanden.

7. Respektera din familjs och dina vänners inställning till sociala medier. Även om du själv är intresserad av dem är inte alla det. Om dina närstående inte vill att du ska lägga upp bilder eller information om dem på sociala medier ska du följa deras önskemål. Låt inte heller någon tjänst (på de sociala medierna) ladda ner till exempel din smarttelefons kontakter till tjänsten, om inte din organisations anvisningar tillåter det. Överväg också detta i fråga om dina enheter på fritiden om du vill överlämna alla kontaktuppgifter i telefonen till tjänsten om du inte nödvändigtvis vet med säkerhet hur tjänsten hanterar och utnyttjar dessa uppgifter.

8. Var försiktig när personer som du inte känner vill nätverka med dig. Lita inte enbart på att någon annan i ditt nätverk redan har godkänt personen i fråga.

9. Behandla inte sekretessbelagda uppgifter eller personuppgifter i sociala medier eller i privata meddelanden. Kom ihåg att tjänstens administratörer har tillgång till all information som sparats på tjänsten, även sådan som är avsedd bara för samtalsparterna.

10. Kontrollera innehållet innan du delar information i sociala medier. Lita inte bara på meddelandets rubrik. Innan du delar information som andra producerar i sociala medier ska du se till att du har läst den och vet vad som ingår i helheten och vilket syfte meddelandet har Det lönar sig också att meddela om du delar informationen eftersom du är av samma åsikt eller eftersom du vill lyfta fram information som avviker från din egen synvinkel. Likaså lönar det sig att på förhand bedöma vilka reaktioner budskapet kan väcka och delvis förbereda sig på responsen. Särskilt Twitter är känslig för att "flamma upp".

11. Om du är osäker på informationens äkthet är det bra att kontrollera om saken rapporteras även i andra nyhetskällor. Om saken inte nämns i andra medier kan man misstänka att nyheten är sanningsenlig och det finns skäl att noggrant överväga om det lönar sig att sprida meddelandet vidare.

12. Försök lägga märke till om någon försöker påverka dig. När det är bråttom är det inte så lätt att lägga märke till exempelvis dold kommunikation eller andra påverkningsmetoder som riktas till oss. Med hjälp av sådan kan man försöka påverka dina känslor, tankar, attityder, beslut och därigenom ditt beteende.

5. Hur kan jag lära mig mer?

Nu, när du har läst det här stödmaterialet och förverkligat den goda praxis som presenteras här, har du goda grunder för att arbeta säkert. Du kan studera vidare genom följande webbutbildningar om det digitala livet:

Digital säkerhet i arbetslivet
https://www.eoppiva.fi/koulutukset/digiturvallinen-tyoelama/

Agera säkert i den digitala världen

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

Digital säkerhet för kommunernas förtroendevalda

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

Dessutom kan du öva och repetera det du lärt dig genom att ladda ner spelet Digiturvallinen elämä som Myndigheten för digitalisering och befolkningsdata producerat. Spelet finns i applikationsbutiken. Det tar ungefär en timme att spela hela spelet. År 2021 publiceras minst ett uppdateringspaket för spelet.

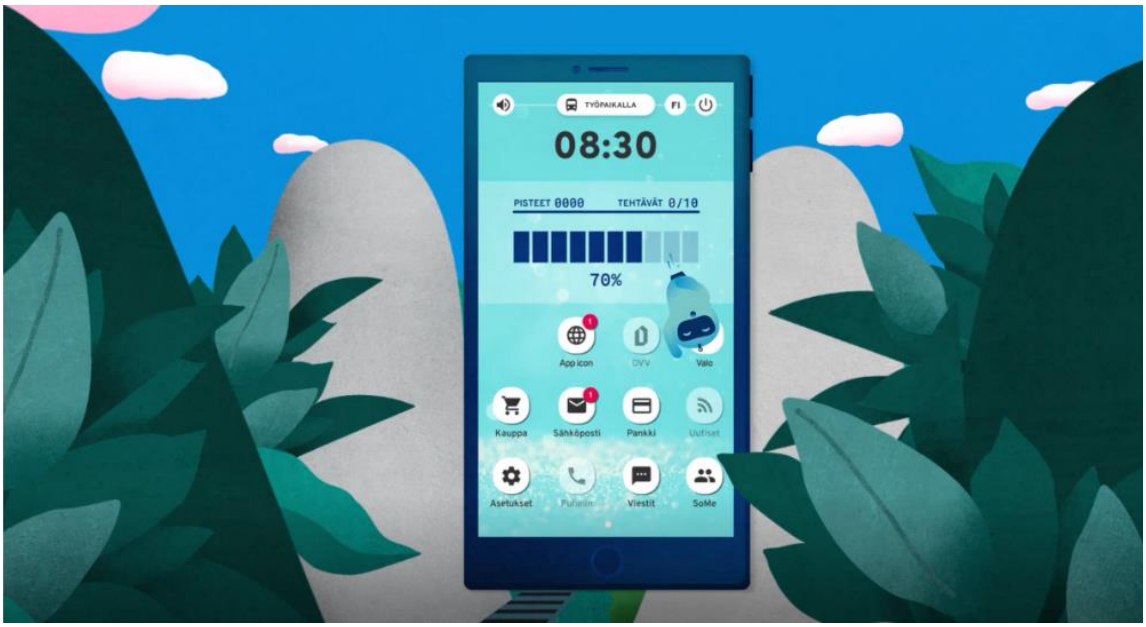

Bild 6. Digiturvallinen elämä lär dig hur du ska agera tryggt i den digitala världen genom att öva på hot som arbetstagare i den fiktiva kommunen Tyrskylä stöter på.