Kyberturvallisuutta sosiaali- ja terveysalan ammattilaisille 3 op (avoimet oppimateriaalit)

Sisällysluettelo

Sivun 2 lähteet:

- Blek, T. & Solankallio-Vahteri, T. 2022. Terveydenhuollon hoitohenkilöstön tieto- ja kyberturvallisuusosaaminen. FinJeHeW 14 (4): 352–363
- Rajamäki, J., Rathod, P. & Kioskli, K. 2023. Demand analysis of the cybersecurity knowledge areas and skills for nurses: Preliminary findings. Proceedings of the 22nd European Conference on Cyber Warfare and Security, ECCWS: 711–716.

1 Johdanto

Tässä dokumentissa kuvattu opintojakso/koulutus on toteutettu osana Jatkuvan oppimisen ja työllisyyden palvelukeskuksen (Jotpa) rahoittamaa Kyberturvallisuutta sosiaali- ja terveysalan ammattilaisille -hanketta. Toteuttajana oli Jyväskylän ammattikorkeakoulu. Tavoitteena hankkeessa oli sosiaali- ja terveysalalla työskentelevien ammattilaisten kyberturvallisuusosaamisen kehittäminen. Lisäksi hankkeessa arvioitiin koulutukseen osallistuneiden osaamisen kehittymistä tutkimuksessa, jonka tulokset on julkaistu toisaalla.

Hankkeessa kehitettiin ja pilotoitiin sosiaali- ja terveysalan ammattilaisille suunnattu kyberturvallisuuskoulutus (koulutukseen osallistumisen edellytyksenä oli sosiaali- ja terveysalan taustakoulutus tai työ sote-alan organisaatiossa, mikä varmistettiin ilmoittautumisen yhteydessä). Koulutus järjestettiin non-stop toteutuksena Moodle verkko-oppimisympäristössä 1.3.2023–31.3.2024. Koulutus toteutettiin verkko-opintoina, ja opiskelijan eteneminen opinnoissa oli täysin ajasta ja paikasta riippumatonta. Koulutuksen laajuus oli kolme opintopistettä, mikä vastaa noin 81 h opiskelijan työtä. Koulutus oli EFQ6 -tasoinen.

Pilotin jälkeen koulutuksen suorittaneilta opiskelijoilta (n = 40) saatu palaute analysoitiin ja koulutusta jatkokehitettiin palautteen pohjalta. Tässä dokumentissa kuvataan koulutus kokonaisuudessaan tavoitteiden, sisältöjen, oppimateriaalien, tehtävien sekä pedagogisen käsikirjoituksen osalta.

2 Hankkeen aikana järjestetyn pilottikoulutuksen tiivis kuvaus

Koulutuksen tavoitteena oli, että sen suoritettuaan opiskelijat ymmärtävät kyberturvallisuuden merkityksen sosiaali- ja terveysalalla, tunnistavat oman roolinsa sosiaali- ja terveysalan kyberturvallisuuden edistämisessä, osaavat toimia kyberturvallisesti sosiaali- ja terveysalan toimintaympäristöissä sekä tietävät henkilötietojen käsittelyn ja informaatiolukutaidon periaatteita.

Koulutus muodostui kuudesta eri sisältöosiosta: johdanto kyberturvallisuuteen, kyberturvallisuus sosiaali- ja terveysalalla sisältäen mm. kyberuhkiin liittyvän oppimateriaalin, lääkinnällisten laitteiden kyberturvallisuus, työntekijän rooli kyberturvallisuuden varmistamisessa, tietosuoja sosiaali- ja terveysalalla sisältäen mm. tutustumisen GDPR-asetukseen, sekä informaatiovaikuttaminen. Sisällöt valikoitiin teoriatietoon perustuen. Esimerkiksi Blek &

Solankallio-Vahteri 2022 havaitsivat tutkimuksessaan, että hoitohenkilöstöllä on puutteellinen tietämys GDPR-asetuksen ja informaatiovaikuttamisen osalta (Blek & Solankallio-Vahteri 2022), joten myös nämä huomioitiin koulutussisällöissä. Muut sisällöt valittiin sote-henkilöstölle tunnistettujen osaamistarpeiden perusteella (mm. Rajamäki ym. 2023).

Osioiden sisällöt rakentuivat erilaisista oppimateriaaleista: videomuotoisista luentotallenteista sekä avoimesti saatavilla olevasta muusta materiaalista (esim. podcast tai tapauskuvaus). Osa oppimateriaaleista oli tekstimuodossa (esim. osioiden aihealueisiin liittyvät artikkelit). Opiskelija ohjeistettiin tekemään jokaisen opiskeltavan osion lopuksi muistiinpanoja. Opiskelijoilla oli mahdollisuus keskustella koulutuksen teemoista muiden opiskelijoiden kanssa verkko-oppimisympäristöön rakennetulla keskustelualueella.

Arvioitavina oppimistehtävinä opiskelija vastasi koulutuksen päätteeksi monivalintatenttiin sekä reflektoi osaamistaan omin sanoin ennalta määritettyjen kysymysten pohjalta. Reflektiotehtävästä opiskelija sai opettajalta henkilökohtaisen palautteen.

3 Kyberturvallisuutta sosiaali- ja terveysalan ammattilaisille 3 op (EFQ6-tasoinen koulutus) – Ohjeet opintojakson rakentamiseen

Tässä osiossa kuvaamme, miten olemme rakentaneet opintojakson. Opintojaksoa on testattu pilottikoulutuksessa (ks. edellinen luku) ja jatkokehitystyössä on huomioitu siitä saatu opiskelijapalaute (n = 40).

3.1 Rakenne

Kaikki opintojakson sisällöt ovat työtilassa (esim. Moodle) osioittain, jolloin yhden osion alla on kyseiseen sisältöalueeseen liittyvät oppimateriaalit ja osion lopussa myös monivalintatesti osion ydinasioista, millä testataan oppijan osaamista. Osiot muodostuvat sisältöalueiden mukaisesti (kaikkiaan kuusi sisältöaluetta = kuusi osiota) ja opiskelijalle suositellaan, että hän suorittaisi ne numerojärjestyksessä. Osioiden oppimateriaali on monimuotoista: videoita ja luettavia materiaaleja. Opiskelijaa on tärkeää ohjata tekemään osioista itselleen muistiinpanoja.

Sisältöosioiden lisäksi opintojaksolla on seuraavat osiot:

- Tervetuloa (ennen sisältöosioita)
    - Alussa tiivis ohjevideo opiskelijalle, missä esitellään opintojakson opettaja/opettajat, kerrotaan opintojakson tavoitteet, työmäärä ja sen jakautuminen, hyväksytyn suorituksen kriteerit sekä esitellään, miten oppimisympäristössä navigoidaan ja miten opettajaan otetaan yhteyttä tarvittaessa.
    - Lyhyesti kirjallisessa muodossa seuraavat asiat: opintojakson osaamistavoitteet (ks. kohta 3.2), opintojakson sisällöt (ks. kohta 3.3), työmäärä ja sen jakautuminen (ks. kohta 3.5), ohjaus opintojaksolla (miten opiskelija saa ohjausta opettajalta, ks. kohta 3.6), arviointi (ks. kohta 3.7) sekä opintojakson eteneminen (ks. kohta 3.9)
- Sisältöosiot (kuusi kappaletta, esitellään yksityiskohtaisemmin omassa luvussaan)
- Tehtävät
    - Osio, mistä löytyvät kaikki tehtävät kootusti (osaamistestit ja reflektio/soveltava tehtävä)
- Materiaalit
    - Opintojakson keskeiset artikkelit / muu kirjallisuus, podcastit, verkkokoulutukset (eriteltynä must know -materiaali / nice to know -materiaali)

3.2 Tavoitteet

- Ymmärrät kyberturvallisuuden merkityksen sosiaali- ja terveysalalla
- Tunnistat oman roolisi sosiaali- ja terveysalan kyberturvallisuuden edistämisessä
- Osaat toimia kyberturvallisesti sosiaali- ja terveysalan toimintaympäristössä
- Tiedät henkilötietojen käsittelyn ja informaatiolukutaidon periaatteita

3.3 Sisältö

- Kyberturvallisuuden merkitys sosiaali- ja terveysalan toimintaympäristössä
- Kyberturvallisuusuhat sosiaali- ja terveysalalla
- Työntekijän rooli kyberturvallisuuden varmistamisessa (ennaltaehkäiseminen ja häiriötilanteessa toimiminen)
- Henkilötietojen käsittely sosiaali- ja terveysalalla

- Informaatiovaikuttaminen ja sen tunnistaminen

3.4 Toteutustapa

Opintojakso järjestetään nonstop -toteutuksena (sai paljon positiivista palautetta opiskelijoilta) = täysin ajasta ja paikasta riippumatonta opiskelua opintojakson suoritusajan puitteissa.

3.5 Opintojakson kuormittavuus

Opintojakson laajuus on 3 op, joka vastaa 81 tuntia opiskelijan työtä. Työmäärä jakaantuu seuraavasti:

- Itsenäinen opiskelu 67 (2,5 op) tuntia (tallennetut luennot ja materiaaliin perehtyminen)
- Tehtävät 14 (0,5 op) tuntia (lopputesti ja reflektiotehtävä)

3.6 Ohjaus

Opiskelija suorittaa opintojakson täysin itsenäisesti aikaan ja paikkaan sitomattomasti. Opintojakson vastuullisen opettajan/opettajien on kuitenkin tärkeä tarjota väylä, mitä kautta opettajan ohjausta on mahdollista saada.

Esimerkki ohjausväylistä, joita käytimme pilottikoulutuksessa ja joita pidimme toimivina

”Mikäli haluat opettajilta ohjausta opintojakson suorittamiseen liittyen, käytä hyväksesi Moodlen "Kysy opettajalta!" -keskustelualuetta. Henkilökohtaisissa asioissa voit myös olla yhteydessä opettajiin sähköpostitse.”

3.7 Arviointi

Arviointi tehdään asteikolla hyväksytty/hylätty. Hyväksytyn suorituksen edellytyksenä on, että opintojakson tehtävät on suoritettu hyväksytysti opintojakson päättymiseen mennessä.

3.8 Opintojakson arvioitavat tehtävät

3.8.1 Monivalintatestit

Pienet osaamistestit sisältöosioiden päätteeksi

Opintojaksolla osaamisen arviointiin soveltuvia tehtäviä ovat osaamistestit, missä hyödynnetään monivalintakysymyksiä. Osaamistesti sijoitetaan (n. 5 kysymystä) jokaisen sisältöalueen (osion) päätteeksi, jolloin testiin rakennetaan monivalintakysymyksiä kyseisen sisältöalueen ydinasioista. Pilottikoulutuksessa käytimme hyväksytyn osaamistestin rajana 80 % maksimipisteistä.

Kokoava lopputesti (tarvittaessa)

Osaamista voi tarvittaessa arvioida myös lopputestissä, jossa monivalintakysymykset on koostettu kaikista kuudesta sisältöosiosta samaan lopputestiin (25–30 kysymystä). Mikäli lopputestiä käytetään, suosittelemme, että siitä huolimatta hyödynnetään myös pieniä osaamistestejä jokaisen sisältöalueen (osion) päätteeksi, jolloin lopputesti voidaan kasata siten, että siinä on satunnaisessa järjestyksessä samoja monivalintakysymyksiä kuin pienissä osaamistesteissä. Tällöin pienet osaamistestit voivat toimia opiskelijalle harjaannuttavana ja kertausta tukevana elementtinä, ja kokoava lopputesti on se, minkä pohjalta arviointi tehdään.

3.8.2 Osaamisen reflektio/soveltava tehtävä

Monivalintatestien lisäksi kyberturvallisuuskoulutukseen sisällytetään tehtävä, jossa opiskelija reflektoi / soveltaa oppimaansa. Reflektio / soveltavan tehtävän arviointikriteerejä on hyvä pohtia: riittääkö, että tehtävä on tehty vai onko sille erilliset arviointikriteerit. Pilottikoulutuksessamme hyväksyttyyn suoritukseen riitti, että opiskelija on vastannut reflektiotehtävään ja varsinainen osaamisen arviointi tehtiin osaamistestin (ks. yllä) perusteella. Opiskelijat odottavat saavansa palautetta reflektiostaan / soveltavasta tehtävästään, joten suosittelemme, että opiskelijalle sitä annetaan hänen vastauksensa pohjalta (ovatko asiat hallussa vai ei ja miten osaamisen jatkokehittämistä olisi hyvä tehdä).

Esimerkki reflektiotehtävästä

Kysymykset:

- *Miksi sinun mielestäsi huomion kiinnittäminen sosiaali- ja terveysalan kyberturvallisuuteen on tärkeää? (pakollinen kysymys)*
- *Mitä sosiaali- ja terveysalan ammattilaisen tulisi mielestäsi osata alan kyberturvallisuuden vahvistamiseksi? (pakollinen kysymys)*
- *Kuvaa lyhyesti keskeiset oppimiskokemuksesi tältä opintojaksolta (pakollinen kysymys)*
- *Kerro vapaasti, mitä mieltä olit opintojakson toteutuksesta. Missä onnistuimme, missä meillä on vielä kehitettävää? (vapaaehtoinen kysymys)*

Esimerkki soveltavasta tehtävästä (ei kokeiltu pilottijaksolla, mutta vinkattu opiskelijoille reflektiotehtävän palautteen yhteydessä):

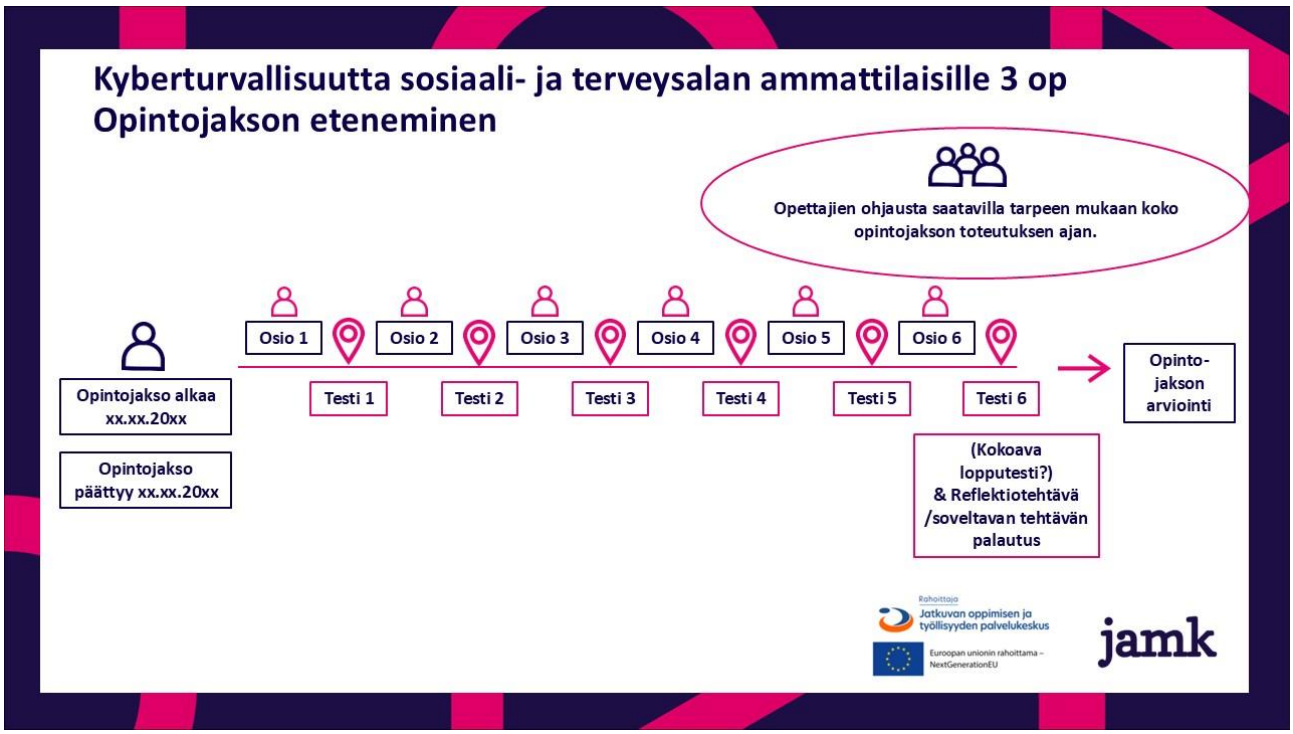
Lähde havainnoimaan ympäristöösi. Jos olet tällä hetkellä töissä sote-alan organisaatiossa, toiminnan havainnoiminen omalla työpaikallasi voi tuoda mielenkiintoisia oivalluksia. Havainnoi vähintään 2-3 päivän ajan, millaisia kyberturvallisuusriskejä havaitset työpaikallasi. Voit tarkastella mm. seuraavia asioita:

- *Pidetäänkö salasanat huolellisesti omana tietona (vai keskustellaanko niistä tai onko niitä yleisesti esillä)?*
- *Käytetäänkö henkilökohtaisia käyttäjätunnuksia/varmennekorttia kirjauduttaessa koneelle/järjestelmiin (vai onko käytössä yhteiskäyttötunnuksia tai annetaanko toisten kirjautua omilla tunnuksilla)?*
- *Kirjaudutaanko yhteiskäyttöisiltä tietokoneilta ulos käytön jälkeen?*
- *Lukitaanko henkilökohtaisessa käytössä oleva tietokone silloin, kun se ei ole koneen käyttäjän välittömässä valvonnassa?*
- *Onko laitteiden ja sovellusten päivitykset kunnossa?*
- *Ovatko käytössä olevat lääkinnälliset laitteet kohtalaisen uusia ja päivitettyjä? Onko laitteilla joku, joka vastaa niistä?*
- *Liitetäänkö työtietokoneisiin vain työkäytössä olevia muistitikkuja/ulkoisia laitteita (vai myös henkilökohtaisia muistitikkuja, puhelimia)?*
- *Lähetetäänkö asiakkaan tai potilaan henkilötietoja vain turvasähköpostilla (vai käytetäänkö myös suojaamattomia sähköpostiviestejä)? Käsitelläänkö asiakkaan/potilaan henkilötietoja Whatsappissa?*
- *Onko työntekijöillä aikaa pysähtyä ja keskittyä esimerkiksi sähköpostien lukemiseen (vai tehdäänkö asiat kiireellä)?*
- ***Onko organisaatiosi tietoturvaohjeet helposti saatavilla? Selvitä, mistä ne löytyvät ja tutustu niihin.***

- *Tiedetäänkö työpaikallasi, kuinka häiriötilanteissa toimitaan, jos esimerkiksi asiakas- ja potilastietojärjestelmä tai jokin muu tietojärjestelmä ei toimi?*
- *Onko asiakkaiden tai potilaiden paperit/henkilötiedot pois näkyviltä ja ulkopuolisten saavuttamattomissa työpaikkasi tiloissa (vai avoimesti näkyvillä)?*
- *Pääseekö työpaikkasi henkilökunnalle tarkoitettuihin työskentelytiloihin vain sinne kuuluvat henkilöt (vai voisiko joukkoon livahtaa helposti myös ulkopuolinen)?*

3.9 Opintojakson eteneminen (opiskelijan polku)

Opiskelijan eteneminen opintojaksolla esitetään oppimisympäristössä visuaalisessa muodossa (ks. esimerkkikuva alla). Lisäksi opiskelijan tukena hyödynnetään edistymisen seurantaa (Moodlen edistymisen seuranta -lohko), mistä opiskelija voi nähdä yhdellä silmäyksellä sekä opiskeltavat osiot että tehtävät, mitkä hänen on tehtävä, jotta voi saada hyväksytyn suorituksen. Edistymisen seurannan hyödyllisyyden kannalta on keskeistä, että opiskelija voi nähdä oman edistymisensä esimerkiksi merkkaamalla sisältöosion tehdyksi, kun hän on sen opiskellut. Pilottikoulutuksessa rakensimme edistymisen seurannan palkin siten, että yksi palkki vastasi kutakin sisältöosiota tai tehtävää.



3.10 Opintojakson sisällöt

Opintojakson tarkemmat sisällöt ja luentomateriaalit löytyvät liitteistä sisältöosioittain.

4 Opintojaksopalautteesta opitut vinkit

4.1 Yhteisöllisyys toisten opiskelijoiden kanssa opintojakson aikana

Pilottikoulutuksessa jokaisen osion päätteeksi oli linkki keskustelualueelle, jossa opiskelijoiden oli mahdollista keskustella toistensa kanssa opintojakson herättämistä ajatuksista/kysymyksistä. Keskustelualue on kuitenkin haastava saada toimimaan nonstop-toteutuksella, koska opiskelijat opiskelevat omaan tahtiinsa. Pilottikoulutuksessa keskustelualuetta hyödynnettiin melko vähän (4/40 opiskelijan toimesta). Keskustelualueen tarpeellisuus myös kyseenalaistettiin yhdessä opintojaksopalautteessa. Näiden syiden vuoksi jätimme keskustelualueen pois lopullisesta toteutuskuvauksesta, minkä olemme kuvanneet aiemmin. Kenties vaihtoehtona keskustelualueelle voisi toimia noin 30 minuutin mittaiset keskusteluillat, joita markkinoitaisiin hyvin jo opintojakson alussa.

Ohjeet, jotka annoimme opiskelijoille keskustelualueen hyödyntämiseen pilottikoulutuksessa (hyödynnä tarvittaessa)

Opintojakson alussa: *”Jokaisen osion päätteeksi on mahdollista käydä keskustelua opiskelijakollegoiden kanssa sivun alalaidasta löytyvällä keskustelualueella. Keskusteleminen opiskelijakollegoiden kanssa ei ole pakollista opintojakson suorittamisen kannalta, mutta keskusteluun osallistumista suositellaan, sillä usein keskustelun myötä myös oma ymmärrys aiheesta lisääntyy. Huomioithan, että opiskelijat voivat edetä opintojaksolla hyvin eri aikaisesti, joten keskustelu ei välttämättä tapahdu reaaliaikaisesti.”*

Jokaisen osion päätteeksi: ” ***Herättikö teema ajatuksia?*** *Keskustele niistä opiskelijakollegoidesi kanssa täällä (hyperlinkki). Keskusteluun osallistuminen on vapaaehtoista eikä ole edellytys opintojakson suorittamiselle.”*

4.2 Opiskelijan osaamisen arvioiminen

Pilottikoulutuksessa opiskelijan osaamista arvioitiin lopputestissä (25 kysymyksen monivalintatesti opintojakson jokaisen kuuden sisältöalueen (osion) ydinasioista. Opiskelijapalautteeseen perustuen jatkokehitimme tätä ratkaisua. Lopullisessa toteutuskuvauksessa (ks. luku 3) lopputesti pilkotaan

pienempiin osaamistesteihin (kuusi kappaletta), jotka löytyvät jokaisen osion lopusta. Näin saadaan osaamista testattua pienempänä kokonaisuutena ja opiskelija voi tarvittaessa palata kertaamaan oppimateriaaleja, mikäli jonkin sisällön osalta havaitaan vielä puutteita. Osaamistesti on siis samalla osion ydinsisältöjen kertausta.

Tarvittaessa opintojakson loppuun voi lisätä kaikki sisältöalueet kokoavan lopputestin, jossa on satunnaisesti valikoituna niitä kysymyksiä, mitä jo jokaisen osion päätteeksi olleissa pienemmissä osaamistesteissä on ollut. Mikäli lopputestiä käytetään, opiskelija on tärkeä ohjata tekemään se vasta sen jälkeen, kun hän on opiskellut opintojakson kaikki sisältöalueet.

4.3 Oppimateriaalien monimuotoisuus ja videoluennot

Opiskelijoiden antaman palautteen perusteella voimme todeta, että opintojaksolla on tärkeää hyödyntää monimuotoisia oppimateriaaleja, kuten videoita ja luettavia materiaaleja. Hyödynsimme pilottikoulutuksessa luentoja, jotka olivat videotallenteina oppimisympäristössä. Palautteen perusteella näistä pidettiin todella paljon (useita myönteisiä palautteita liittyen videotallenteisiin). Luentodiat löytyvät liitteistä.

Pilottikoulutuksessa luentojen videotallenteet olivat kestoltaan n. 30 minuuttia/luento. Palautteen perusteella yhden sisältöosion luento voisi olla järkevä pilkkoa vieläkin pienempiin osioihin, sillä silloin mahdollistamme opiskelijalle opiskelun myös esimerkiksi lyhyemmän tauon aikana. Lopullisessa toteutuskuvauksessa olemme merkinneet materiaaleihin, mistä kohti kunkin sisältöalueen luentomateriaalit on järkevä jakaa, mikäli luennoista halutaan tehdä lyhyitä, n. 5-10 minuutin videotallenteita.

Koska opiskelijat ovat erilaisia, ”one size fits for all” ei useinkaan ole se paras vaihtoehto ja tämä tuli ilmi myös opiskelijapalautteessa eli vaikka videoista valtaosin pidettiin, toivottiin myös, että videoiden sijaan materiaalit olisi luettavassa muodossa. Tämän vuoksi luennoista tehtyjen videotallenteiden lisäksi oppimisympäristöön kannattaa viedä myös luentomateriaalit luettavassa muodossa (esim. PowerPoint diat).

4.4 Opintojaksopalautteen kokonaiskuva

Pilottikoulutuksen opiskelijoilta saadut pääasialliset kehittämisehdotukset on tuotu esiin luvuissa 4.1–4.3). Kokonaisuudessaan voi sanoa, että pilottikoulutuksesta saatu palaute oli varsin myönteistä ja useampi vastaaja toi avoimessa palautteessaan esiin, että jokaisen sote-alalla työskentelevän olisi hyvä käydä tällainen koulutus.

Liite 1. Sisältöosiot: 1. Johdanto kyberturvallisuuteen

Merkitse tehdyksi

1 Johdanto kyberturvallisuuteen

1. Tutustu alla olevan tekstin ja videon myötä siihen, mitä digitaalisella turvallisuudella ja kyberturvallisuudella tarkoitetaan.
2. Tee kuulemastasi ja lukemastasi muistiinpanoja. Tarvitset niitä sekä opintojakson lopputestissä että reflektiotehtävässä.

Mitä digitaalisella turvallisuudella ja kyberturvallisuudella tarkoitetaan?

Digitaalinen turvallisuus koostuu viidestä osa-alueesta, joita ovat toiminnan jatkuvuus ja varautuminen, riskienhallinta, tietosuoja, tietoturva ja kyberturvallisuus (eOppiva n.d.)

Hallitsemalla digitaalisen turvallisuuden perusteet osaat toimia vastuullisesti ja turvallisesti sekä vähentää erilaisten poikkeamien ja häiriöiden todennäköisyyttä ja vaikutusta. Kehitä siis turvallisuutta ja ylläpidä luottamusta (eOppiva n.d.)

- Omaan toimintaasi
- Organisaatiosi toimintaan
- Kansalaisiin, asiakkaisiin/potilaisiin ja muihin sidosryhmiin

Sinulla on tärkeä rooli näiden osa-alueiden toteuttajana!

Tietosuojalla tarkoitetaan järjestelyjä, joilla pyritään varmistamaan henkilötietojen asianmukainen käsittely ja niiden yksityisyyden säilyminen. Henkilötietosuoja pyritään toteuttamaan mm. tietoturvalla. (Kyberturvallisuuden sanasto 2018.)

Tietoturvalla tarkoitetaan järjestelyjä, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus (Kyberturvallisuuden sanasto 2018).

- Saatavuus = tieto on hyödynnettävissä silloin, kun halutaan.
- Eheys = tieto on yhtäpitävä alkuperäisen tiedon kanssa eli tieto ei ole muuttunut
- Luottamuksellisuus = kukaan sivullinen ei saa tietoa

Kyberturvallisuudella tarkoitetaan digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin. Kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia. (Kyberturvallisuuden sanasto 2018.)

Suomen kyberturvallisuusstrategiassa määritellään keskeiset tavoitteet ja toimintalinjat, joiden avulla Suomi vastaa kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistaa sen toimivuuden (valtioneuvoston periaatepäätös 24.1.2013).

Videolla Kyberturvallisuuskeskuksen ylijohtaja, Kalle Luukkainen, kertoo käytännönläheisesti, mitä kyberturvallisuus tarkoittaa:

Linkki videoon (#tietoturvatorstai: Mitä on kyberturvallisuus)

https://www.youtube.com/watch?v=W8b9SuGBrEc

"Hyvinkin moni yhteiskunnan toiminnoista on hyvin nopeassa ajassa nurin, jos tietojärjestelmät eivät toimi." Kalle Luukkainen, Ylijohtaja, Kyberturvallisuuskeskus

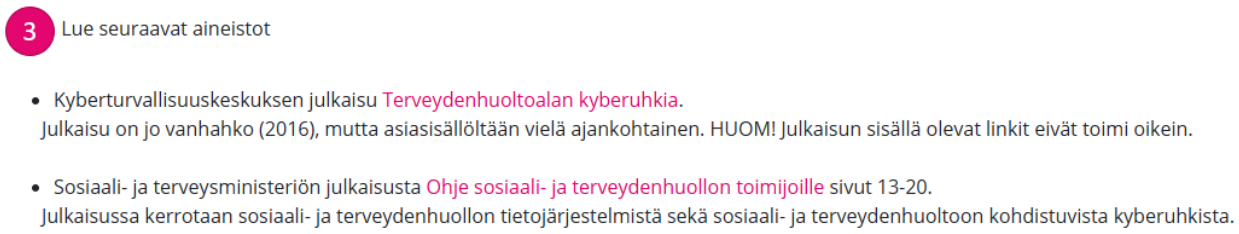
Herättikö teema ajatuksia? *Keskustele niistä opiskelijakollegoidesi kanssa täällä. Keskusteluun osallistuminen on vapaaehtoista eikä ole edellytys opintojakson suorittamiselle.*

Liite 2. Sisältöosiot: 2. Kyberturvallisuus sosiaali- ja terveysalalla

Kohdan 1 luentomateriaali pdf-muodossa erillisenä tiedostona.

Linkit tapauskuvauksiin:

- Lahden kaupungin kokemuksia kyberhyökkäyksestä: https://www.youtube.com/watch?v=K8mqA94RVQ4
- Ylen artikkeli (9.12.2022): Sähköiset reseptit eivät toimi kaikkialla – syynä Kelaan ja Kantaan kohdistuva palvelunestohyökkäys: https://yle.fi/a/74-20008024#:~:text=Palvelunestohy%C3%B6kk%C3%A4ys%20Kelaan%20on%20aiheuttanut%20ongelmia%20l%C3%A4%C3%A4kkeiden%20saannissa.%20Ylen,olla%20hetkellisesti%20tilanteita%2C%20joissa%20l%C3%A4%C3%A4kkeit%C3%A4%20ei%20ole%20saanut.
- Lääkärilehden artikkeli (8.6.2017): WannaCry-haittaohjelma löytyi TYKS:sta: https://www.laakarilehti.fi/ajassa/ajankohtaista/wannacry-haittaohjelma-loytyi-tyks-sta/
- Ylen artikkeli (27.1.2021): Ehkä jopa 32000 Vastaamon potilaan tiedot ilmestyivät viime yönä Tor-verkkoon – poliisi: ”Emme tiedä, monenko käsissä tietokanta on”: https://yle.fi/a/3-11757676
- Liikenne- ja viestintävirasto Traficom. Tietoturvailmiöt, jotka muuttivat maailmaa – Vastaamo: https://youtu.be/0PwnY42dESk



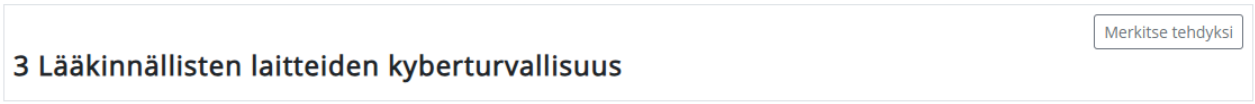
Linkit aineistoihin:

- Kyberturvallisuuskeskuksen julkaisu Terveydenhuoltoalan kyberuhkia: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Terveydenhuoltoalan_kyberuhkia.pdf
- Sosiaali- ja terveysministeriön julkaisu Ohje sosiaali- ja terveydenhuollon toimijoille: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161683/J14_Kyberturvallisuus_WEB.pdf

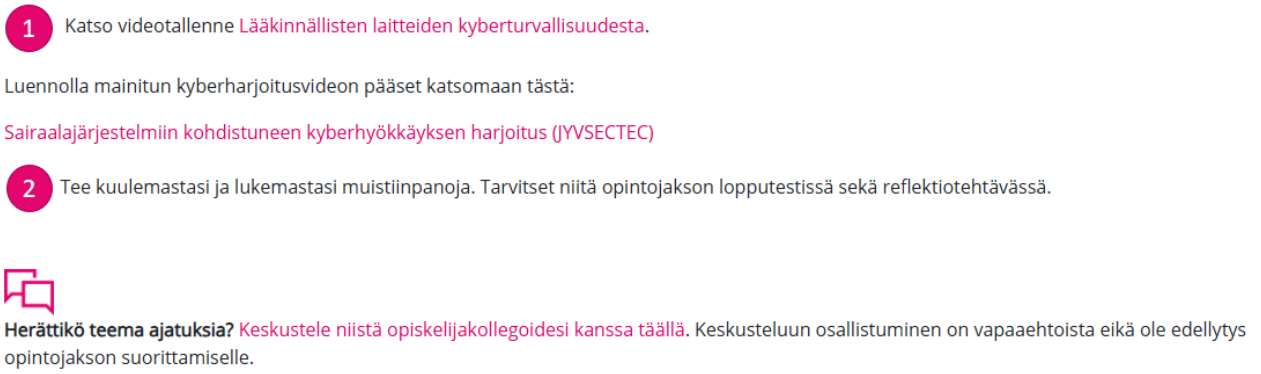
4 Tee kuulemastasi ja lukemastasi muistiinpanoja. Tarvitset niitä sekä opintojakson lopputestissä että reflektiotehtävässä.

Herättikö teema ajatuksia? Keskustele niistä opiskelijakollegoidesi kanssa täällä. Keskusteluun osallistuminen on vapaaehtoista eikä ole edellytys opintojakson suorittamiselle.

Liite 3. Sisältöosiot: 3 Lääkinnällisten laitteiden kyberturvallisuus



Heti osion alkuun video, missä näytetään lääkinnällisen laitteen datan manipulointia. Urgent/11 – Takeovet of a Spavelabs Xprezzon patient monitor: https://www.youtube.com/watch?v=tpSXr4XhQwM



Kohdan 1 luentomateriaali pdf-muodossa erillisenä tiedostona.

Linkki JYVSECTECin videoon: https://jyvsectec.fi/wp-content/uploads/2021/12/HCCR_Pilotti_final_fi_1.3.mp4

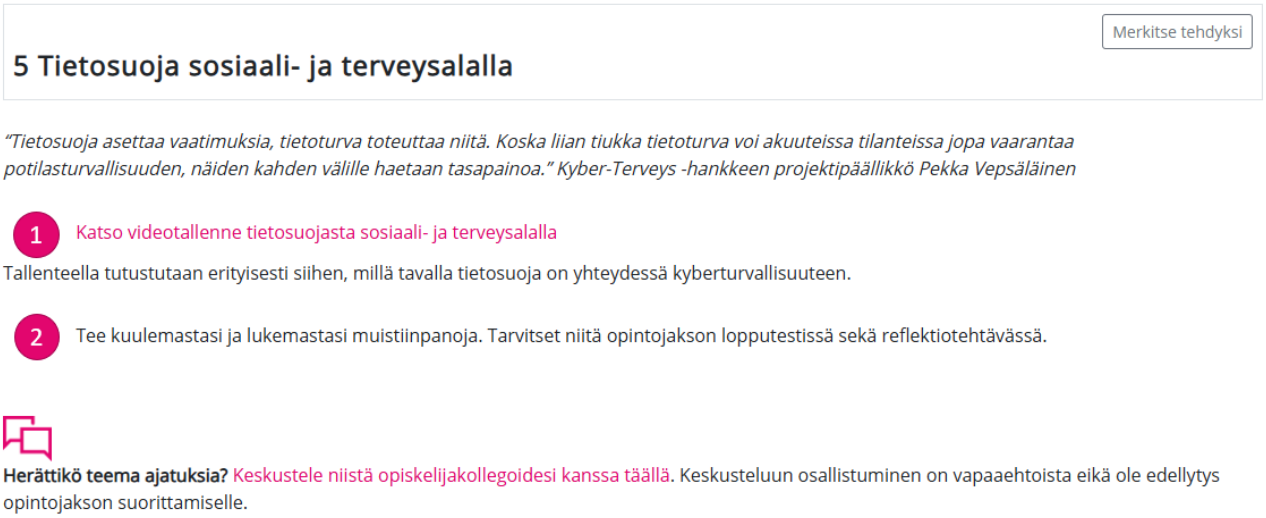
Liite 4. Sisältöosiot: 4 Työntekijän rooli kyberturvallisuuden varmistamisessa

Kohdan 1 luentomateriaali pdf-muodossa erillisenä tiedostona.

Linkit kohdan 2 tutustuttaviin materiaaleihin:

- Ihmispalomuuri organisaation suojana: https://blogit.jamk.fi/cyberdi/2020/05/27/ihmispalomuuri-organisaation-suojana/
- Digiturvallisuuden yleisopas sote-puolelle (Cyberdi-hankkeessa tuotettu, ladattava tiedosto): https://www.jamk.fi/fi/file/cyberdi-digiturvallisuus-sote
- Isännäinen & Tulkki. 2022. Kyberturvallisuus terveydenhuollossa: mitä sairaanhoitajan tulee tietää ja osata (sovellettavissa myös muihin sote-ammattilaisiin kuin sairaanhoitajiin): https://www.theseus.fi/handle/10024/755584
- Blek & Solankallio-Vahteri. 2022. Terveydenhuollon hoitohenkilöstön tieto- ja kyberturvallisuusosaaminen: https://www.theseus.fi/handle/10024/791106

Liite 5. Sisältöosiot: 5 Tietosuoja sosiaali- ja terveysalalla



Merkitse tehdyksi

5 Tietosuoja sosiaali- ja terveysalalla

"Tietosuoja asettaa vaatimuksia, tietoturva toteuttaa niitä. Koska liian tiukka tietoturva voi akuuteissa tilanteissa jopa vaarantaa potilasturvallisuuden, näiden kahden välille haetaan tasapainoa." Kyber-Terveys -hankkeen projektipäällikkö Pekka Vepsäläinen

1 Katso videotallenne tietosuojasta sosiaali- ja terveysalalla

Tallenteella tutustutaan erityisesti siihen, millä tavalla tietosuoja on yhteydessä kyberturvallisuuteen.

2 Tee kuulemastasi ja lukemastasi muistiinpanoja. Tarvitset niitä opintojakson lopputestissä sekä reflektiotehtävässä.

Herättikö teema ajatuksia? Keskustele niistä opiskelijakollegoidesi kanssa täällä. Keskusteluun osallistuminen on vapaaehtoista eikä ole edellytys opintojakson suorittamiselle.

Kohdan 1 luentomateriaali pdf-muodossa erillisenä tiedostona.

Liite 6. Sisältöosiot: 6 Informaatiovaikuttaminen

Merkitse tehdyksi

6 Informaatiovaikuttaminen

Informaatiovaikuttamisella tarkoitetaan kohteelle haitallista toimintaa, jossa informaatiota tuottamalla, muokkaamalla tai sen saatavuutta rajoittamalla pyritään vaikuttamaan kohteen käsityksiin tai toimintaan (Sanastokeskus 2022). Valtioneuvoston kanslian julkaisussa **informaatiovaikuttamisen** määritellään tarkoittavan toimintaa, jolla pyritään vaikuttamaan järjestelmällisesti yleiseen mielipiteeseen, ihmisten käyttäytymiseen ja päätöksentekijöihin sekä sitä kautta yhteiskunnan toimintakykyyn (Valtioneuvoston kanslian julkaisuja 2019:11). Informaatiovaikuttamisen voidaan katsoa kuuluvan myös osaksi kyberturvallisuutta. Verkossa on suunnaton määrä myös terveyteen liittyvää tietoa, minkä vuoksi kenellä tahansa on joskus vaikeuksia erottaa luotettava tieto epäluotettavasta (THL 2022). Tarvitaankin digitaalista informaatiolukutaitoa, jota pidetään yhtenä digiajan kansalaistaidoista (Kivinen ym. 2022)

Digitaalisella informaatiolukutaidolla tarkoitetaan kykyä löytää, saada käyttöönsä, tulkita, analysoida, hallita, ymmärtää, luoda ja levittää informaatiota turvallisesti ja asianmukaisesti sosiaalisessa mediassa digitaalitekniikan avulla. Digitaaliseen informaatiolukutaitoon sisältyy informaatio-, media ja datalukutaitoja, mistä viimeksi mainittu auttaa ymmärtämään digitaalisen infromaatiomaailman toimintaa laajemmin. (Kivinen ym. 2022.)

Informaatiovaikuttamiseen liittyvät keskeisesti myös seuraavat **tietohäiriötyyppien** käsitteet (Kivinen ym. 2022):

- **Misinformaatio** = virheellinen informaatio. Tietoa käytetään väärässä yhteydessä tai sisältö on harhaanjohtava. Tämä voi olla tahatonta eikä aina edes haitallista. Misinformaatiota on myös jaettu sisältö, jonka uskotaan olevan totta, ja joka nähdään tarpeelliseksi julkistaa yhteisen hyvän vuoksi, vaikka sen todenperäisyyttä ei olisikaan tarkistettu.
- **Disinformaatio** = vääristetty informaatio. Tiedon sisältö tai konteksti on tarkoituksellisesti vääristelty mukaan lukien salaliittoteoriat tai muu sisältö, joka voi joissakin tapauksissa olla haitallista.
- **Malinformaatio** = vahingoittava tieto. Väärää sisältöä, joka on tarkoituksellisesti luotu aiheuttamaan vahinkoa tai vaihtoehtoisesti sisältöä käytetään haitallisiin tarkoituksiin.

Tutustu seuraavaksi informaatiovaikuttamiseen ja siihen, miten voit tunnistaa väärän tiedon verkossa.

1

Kohdassa 1 viitataan Liikenne- ja viestintävirasto Traficomin videoon Kyber- ja informaatiovaikuttaminen – mitä minun on hyvä tietää? https://youtu.be/L5oW0MJNZeE

2 Lue THL:n verkkosivuilta, mistä merkeistä voit tunnistaa väärän tiedon verkossa (linkki avautuu uuteen ikkunaan).

3 Tutustu Euroopan parlamentin "Tunnista valeuutiset" -kompassiin (linkki avautuu uuteen ikkunaan).

4 Tee kuulemastasi ja lukemastasi muistiinpanoja. Tarvitset niitä opintojakson lopputestissä sekä reflektiotehtävässä.

Herättikö teema ajatuksia? Keskustele niistä opiskelijakollegoidesi kanssa täällä. Keskusteluun osallistuminen on vapaaehtoista eikä ole edellytys opintojakson suorittamiselle.

Linkit:

- Kohdassa 2 viitattu verkkosivu (THL. Näistä merkeistä tunnistat väärän tiedon verkossa): https://thl.fi/ajankohtaista/tiedotteet-ja-uutiset/naista-merkeista-tunnistat-vaaran-tiedon-verkossa

- Kohdassa 3 viitattu dokumentti (Euroopan parlamentti. Tunnista valeuutiset): https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/599386/EPRS_ATA(2017)599386_FI.pdf