Kyberturvallisuutta sote- ja hoiva-alan opettajille 2 op -verkkokoulutus

Tiina Blek, lehtori Hyvinvointiyksikkö, Jyväskylän ammattikorkeakoulu

Johanna Niskakangas, lehtori, Hyvinvointiyksikkö, Jyväskylän ammattikorkeakoulu

13.3.2025

jamk | Jyväskylän ammattikorkeakoulu University of Applied Sciences

OPETUSHALLITUS RAHOITTAA HANKETTA

Koulutuksen taustatiedot

Koulutus on osa Opetushallituksen rahoittamaa opetustoimen henkilöstökoulutusta.

Kuvaus: Tiesitkö, että potilastiedot ovat ”pimeillä markkinoilla” arvokasta kauppatavaraa? Entä tiesitkö, että valtaosa kyberturvallisuusuhkista johtuu ihmisistä, heidän toiminnastaan ja tietoisuuden puutteesta? Sote-alan ammattilaisilla on keskeinen rooli kyberturvallisuuden varmistamisessa ja siksi meidän opettajien on tärkeä kertoa siitä alalle opiskeleville. Arjen kyberturvallisuus ei vaadi teknistä asiantuntijuutta – se koostuu pienistä, mutta tärkeistä teoista ja tarkkaavuudesta.

Tästä koulutuksesta saat materiaalia (sisältöjä, tehtäväesimerkkejä), jota voit soveltaa omassa opetuksessasi. Koulutuksen sisällöissä keskitytään käsittelemään kyberturvallisuutta sote-alan arjen ja asiakas-/potilastyön näkökulmasta – näkökulma ei ole tekninen.

Kohderyhmä: Toisen asteen, aikuiskoulutuksen ja vapaan sivistystyön opettajat.

OPETUSHALLITUS RAHOITTAA HANKETTA
jamk

Tervetuloa

Tässä koulutuksessa saat ajankohtaista tietoa sosiaali- ja terveysalan kyberturvallisuuteen liittyvistä asioista. Opintojakson sisältö keskittyy alalla työskentelevän henkilöstön arjen kyberturvallisuuteen – lähestymistapa ei ole tekninen.

Koulutuksessa tutustumme erilaisiin kyberturvallisuusuhkiin, jotka kohdistuvat myös sosiaali- ja terveysalaan. Käsittelemme muun muassa:

- Lääkinnällisiin laitteisiin ja potilastietoihin kohdistuvia hyökkäyksiä.
- Identiteettivarkauksia ja tietojen vuotamista.
- Kyberhyökkäysten vaikutuksia potilaiden turvallisuuteen ja terveydenhuollon toimintoihin.
- Kuinka ammattilaiset voivat suojautua ja reagoida kyberuhkiin.

Koulutuksen tavoitteena on tarjota sinulle tietoja ja taitoja, joita voit soveltaa omaan opetustyöhösi.

OPETUSHALLITUS RAHOITTAA HANKETTA
jamk

Tavoitteet ja sisältö

Tavoitteet

- Osaat tunnistaa kyberturvallisuuden tärkeyden osana potilasturvallisuutta
- Osaat arvioida sosiaali- ja terveysalan ammattilaisen kyberturvallisuusosaamisen tarpeita
- Osaat soveltaa sosiaali- ja terveysalan kyberturvallisuustietoja ja -taitoja omaan opetukseesi

Sisältö

- Johdatus kyberturvallisuuteen
- Sosiaali- ja terveysalaan kohdistuvat kyberturvallisuusuhat
- Kyberhyökkäysten vaikutukset potilasturvallisuuteen ja henkilöstöön
- Henkilöstön rooli kyberturvallisuuden varmistamisessa
- Sosiaali- ja terveysalan ammattilaisten kyberturvallisuusosaamistarpeet
- Sovella kyberturvallisuustietoja ja -taitoja kouluttajana

OPETUSHALLITUS RAHOITTAA HANKETTA
jamk

Ohjaus ja oppimistehtävät

Ohjaus

- Ohjausta on tarjolla koko opintojakson ajan. Mikäli haluat opettajilta ohjausta opintojakson suorittamiseen liittyen, hyödynnä keskustelualuetta, jonne löydät linkin infopalkista ("Kysy opettajalta!"). Henkilökohtaisissa asioissa voit myös olla yhteydessä opettajiin sähköpostitse. Lisäksi opintojaksolla järjestetään juttelutuokioita, joihin voit tulla juttelemaan kyberturvallisuuteen liittyvistä teemoista ja kyselemään ohjeistusta opintojaksoon liittyen. Juttelutuokioiden ajankohdat sekä muuta oleellista löydät Juttelutuokiot -välilehdeltä.

Oppimistehtävät

- Oppimistehtäviä on opintojaksolla kaikkiaan kolme: kaksi monivalintatestiä ja yksi soveltava tehtävä. Kaikki oppimistehtävät löytyvät "Oppimistehtävät" -välilehdeltä ja niihin ohjataan myös oikeassa vaiheessa osioiden lopussa. Ensimmäinen testi tehdään osioiden 2-3 ja toinen testi osioiden 4-5 jälkeen. Soveltavan tehtävän osalta tehtävänantoon on tärkeä tutustua heti opintojakson alussa. Suositus on, että työskentelet tämän tehtävän parissa koko opintojakson ajan jo silloin, kun opiskelet eri osioissa käsiteltäviä asioita.

OPETUSHALLITUS RAHOITTAA HANKETTA
jamk

1. Johdatus kyberturvallisuuteen

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 osataan toimia vastuullisesti ja turvallisesti sekä vähentää erilaisten poikkeamien ja häiriöiden todennäköisyyttä ja vaikutusta. Sote-alan ammattilaisen on siis tärkeä kehittää turvallisuutta ja ylläpitää luottamusta (eOppiva n.d.)

- Omaan toimintaan
- Organisaation toimintaan
- Kansalaisiin, asiakkaisiin/potilaisiin ja muihin sidosryhmiin

Sote-alan ammattilaisella 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.)

OPETUSHALLITUS RAHOITTAA HANKETTA
jamk

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.)

Niin sote-alalla kuin muillakin toimialoilla tietoturvan ja -suojan merkitys palveluiden laadulle ja turvallisuudelle on digitaalisessa yhteiskunnassa perusedellytys (Valtioneuvoston julkaisuja 2022: 65).

Suomen kyberturvallisuusstrategiassa määritellään keskeiset tavoitteet ja toimintalinjat, joiden avulla Suomi vastaa kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistaa sen toimivuuden (Valtioneuvoston periaatepäätös 3.10.2019).

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

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

OPETUSHALLITUS RAHOITTAA HANKETTA
jamk

2. Sosiaali- ja terveysalaan kohdistuvat kyberturvallisuusuhat

Sosiaali- ja terveysalan digitalisaatio ja teknologian kehittyminen luovat uusia mahdollisuuksia parempaan potilashoitoon ja tiedonhallintaan. Tämä muutos ei kuitenkaan tule ilman omia haasteitaan. Kyberuhkien määrä ja monimutkaisuus kasvavat jatkuvasti, ja ne voivat vaikuttaa merkittävästi potilasturvallisuuteen ja ammattilaisten toimintaan.

Perehdy sosiaali- ja terveysalaa kohdistuviin kyberuhkiin alla olevan materiaalin avulla:

1. Kuuntele luentotallenne Sosiaali- ja terveysalan kyberturvallisuudesta.
2. Lue julkaisusta Kyberhäiriöiden hallinta - Käsikirja terveydenhuollon toimijoille, sivut 4-13
3. Kuuntele Podcast Kyberrosvot, jakso 6 - Päivä, jona Lahti pysähtyi

Tee opiskellessasi muistiinpanoja tästä osiosta. Muistiinpanoista on apua opintojakson tehtävissä ja erityisesti soveltavassa tehtävässä, jota suosittelemme työstämään koko opintojakson ajan ja viimeistelemään opintojakson päätteeksi. Soveltavan tehtävän tehtävänantoon on siis tärkeä käydä tutustumassa jo tässä vaiheessa välilehdellä "Oppimistehtävät", jos et ole sitä vielä tehnyt. Aloita tehtävän työstäminen ajoissa!

OPETUSHALLITUS RAHOITTAA HANKETTA
jamk

3. Kyberhyökkäysten vaikutukset potilaisiin ja henkilöstöön

Kyberhyökkäyksellä on laajat vaikutukset organisaation toimintaan, potilaiden turvallisuuteen sekä henkilöstön työskentelyyn. Vaikutukset ovat riippuvaisia hyökkäystavasta (esim. kiristyshaittaohjelma vs. tietomurto).

1. Tutustu luentomateriaaliin Kyberhyökkäysten vaikutukset potilasturvallisuuteen ja henkilöstöön.
2. Lue artikkeli Irlannissa tapahtuneen laajan kyberhyökkäyksen vaikutuksista henkilöstön työskentelyyn. Artikkeli on englanninkielinen.

Tee opiskellessasi muistiinpanoja tästä osiosta. Muistiinpanoista on apua opintojakson tehtävissä ja erityisesti soveltavassa tehtävässä, jota suosittelemme työstämään koko opintojakson ajan ja viimeistelemään opintojakson päätteeksi.

OPETUSHALLITUS RAHOITTAA HANKETTA
jamk

4. Henkilöstön rooli kyberturvallisuuden varmistamisessa

1. Kuuntele tallenne sote-henkilöstön rooli kyberturvallisuuden varmistamisessa.
2. Tutustu Cyberdi-hankkeessa toteutettuun digiturvallisuusoppaaseen, joka on suunnattu terveydenhuollon ammattilaisille. Löydät oppaan pdf-muodossa tämän sivun lopusta. Halutessasi voit tutustua myös muihin Cyberdi-hankkeessa tuotettuihin materiaaleihin. Hankkeessa on tuotettu paljon yleistajuista materiaalia kyberturvallisuuteen liittyen.

Tee opiskellessasi muistiinpanoja tästä osiosta. Muistiinpanoista on apua opintojakson tehtävissä ja erityisesti soveltavassa tehtävässä, jota suosittelemme työstämään koko opintojakson ajan ja viimeistelemään opintojakson päätteeksi.

Pääset tutustumaan CYBERDI-hankkeeseen TÄÄLTÄ. Sivustolta saat ladattua digiturvallisuusoppaan!

OPETUSHALLITUS RAHOITTAA HANKETTA
jamk

5. Sosiaali- ja terveysalan ammattilaisten osaamistarpeet

Edellisessä osiossa käsiteltiin henkilöstön roolia kyberturvallisuuden varmistamisessa. Kuten huomasit, myös sote-alan ammattilaiset tarvitsevat kyberturvallisuusosaamista. Kyberturvallisella toiminnalla varmistetaan potilasturvallisuutta. Tässä osiossa tarkastellaan henkilöstön kyberosaamista sosiaali- ja terveydenhuollossa sekä vedetään yhteen sote-ammattilaisten kyberturvallisuusosaamistarpeita.

1. Katso luentotallenne sosiaali- ja terveysalan ammattilaisten kyberturvallisuusosaamistarpeet
2. Lue seuraava artikkeli, jossa käsitellään sosiaali- ja terveysalan ammattilaisten osaamistarpeita: 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 22(1): 711–716. Artikkeli on englanninkielinen.

Tee opiskellessasi muistiinpanoja tästä osiosta. Muistiinpanoista on apua opintojakson tehtävissä ja erityisesti soveltavassa tehtävässä, jota suosittelemme työstämään koko opintojakson ajan ja viimeistelemään opintojakson päätteeksi.

OPETUSHALLITUS RAHOITTAA HANKETTA
jamk

6. Sovella kyberturvallisuustietoja ja -taitoja kouluttajana

Olet nyt opiskellut opintojakson kaikki osiot. Olemme käsitelleet opintojaksolla sosiaali- ja terveysalaan kohdistuvia kyberuhkia, kyberhyökkäysten vaikutuksia potilasturvallisuuteen ja henkilöstöön, henkilöstön roolia kyberturvallisuuden varmistamisessa sekä sosiaali- ja terveysalan ammattilaisten osaamistarpeita. Toivottavasti opintojaksolta on jäänyt käteen paljon uusia oppeja ja oivalluksia tai ainakin aiemmat käsitykset ovat vahvistuneet.

Kuten varmasti huomasit, sosiaali- ja terveysalan ammattilaisilla on keskeinen rooli arjen kyberturvallisuuden varmistamisessa. Olennaista on, että kyberturvallisuuden merkitys sosiaali- ja terveysalalla sekä oman roolin tärkeys sen varmistamisessa tunnistetaan. Kyberturvallisuus ei siis ole ainoastaan tietohallinnon tai muun IT-osaston asia vaan kaikkien asia. Huomionarvoista on myös se, että arjen kyberturvallisuus ei vaadi teknistä asiantuntijuutta – se koostuu pienistä, mutta tärkeistä teoista ja tarkkaavuudesta.

Sote-ala on digitalisoitunut viime vuosina nopeaan tahtiin ja digitaaliset työvälineet myös ammattilaisten keskuudessa ovat lisääntyneet. Ei ole myöskään näköpiirissä, että tahti tulisi tästä hidastumaan, päinvastoin (vrt. Valtionneuvoston julkaisuja 2022: 65). Digitalisaatio tuo mukanaan monia hyötyjä, mutta sen myötä ovat lisääntyneet myös mahdollisuudet kyberturvallisuuden vaarantumiselle.

OPETUSHALLITUS RAHOITTAA HANKETTA
jamk

Monin paikoin toisen asteen opetussuunnitelmissa on huomioitu sosiaali- ja terveysalan digitalisoituminen sekä digitaaliset välineet, kuten hyvinvointiteknologiset ratkaisut, ja niiden hyödyntäminen osana työtä. Samalla myös laitteiden turvallista käyttöä on nostettu esiin. On kuitenkin tärkeä kriittisesti arvioida, miten hyvin digitaalista turvallisuutta ja kyberturvallisuutta tällä hetkellä huomioidaan opetussuunnitelmissa ja opetuksessa. Kuten edellisessä osiossa huomasimme, on ammattilaisten kyberturvallisuusosaamisessa edelleen aukkoja, joita on tärkeä pyrkiä paikkaamaan (mm. Blek & Solankallio-Vahteri 2022). Kainiemi ja muut (2023) ovat nostaneet laajan sote-alan ammattilaisille suunnatun (n = 8024) kyselynsä tulosten pohjalta esiin, että tietoturvallisuuden tulisi olla mukana sekä opetussuunnitelmissa että ammattilaisten perehdyttämisessä. Lisäksi Liikenne- ja viestintäministeriön Kyberturvallisuuden kehittämisohjelmassa mainitaan, että turvallinen toiminta digitaalisissa ympäristöissä ja siihen kytkeytyvä osaaminen tulisi integroida opiskeluun ammattialasta riippumatta alaan soveltuvalla tavalla (Paananen 2021). Kyberturvallisuuskoulutuksen suunnittelussa onkin tärkeä huomioida, että se on relevantti, käytännönläheinen ja linjassa niiden uhkien kanssa, mitä eri ammattiryhmät kohtaavat (Jerry-Egemba 2023).

Me sosiaali- ja terveysalan ammattilaisten opettajat olemme tärkeässä roolissa siinä, että pystymme tukemaan opiskelijoidemme kyberturvallisuustietojen ja -taitojen kehittymistä ja siten vahvistamaan heidän työelämätaitojaan. Nyt on siis aika lähteä soveltamaan opintojakson antia käytäntöön! Käytäntöön soveltamista työstetään "Oppimistehtävät" -välilehdeltä löytyvän soveltavan tehtävän kautta, johon pääset myös klikkaamalla alla olevaa linkkiä.

OPETUSHALLITUS RAHOITTAA HANKETTA
jamk

Oppimistehtävät

Testi 1: Testaa osaamistasi osioissa 2–3 oppimasi perusteella.

- Opintojakson ensimmäisessä testissä vastaat monivalinta- tai tosi-epätosi -kysymyksiin. Kysymykset liittyvät osioissa 2–3 käsiteltyihin asioihin. Huomioithan, että monivalintakysymyksissä voi olla yksi tai useampi oikea vastausvaihtoehto. Hyväksytyn suorituksen vaatimuksena on, että 80 % vastauksistasi on oikein.

Testi 2: Testaa osaamistasi osioissa 4–5 oppimasi perusteella.

- Opintojakson toisessa testissä vastaat monivalinta- tai tosi-epätosi -kysymyksiin. Kysymykset liittyvät osioissa 4–5 käsiteltyihin asioihin. Huomioithan, että monivalintakysymyksissä voi olla yksi tai useampi oikea vastausvaihtoehto. Hyväksytyn suorituksen vaatimuksena on, että 80 % vastauksistasi on oikein.

OPETUSHALLITUS RAHOITTAA HANKETTA
jamk

Soveltava tehtävä: Kyberturvallisuusopetusmateriaalin suunnittelu sosiaali- ja terveysalan koulutusohjelmaan

- Tehtävän vaiheet:
  1. Vaihe 1: Tarpeiden arviointi
  2. Vaihe 2: Opetusmateriaalin suunnittelu
  3. Vaihe 3: Opetusmateriaalin toteutus (aikataulu oman harkinnan mukaan)
  4. Vaihe 4: Opetusmateriaalin arviointi ja viimeistely (aikataulu oman harkinnan mukaan)

Palautettava materiaali:

Palauta tehtävänannon kohtien 1–5 mukaisesti luomasi suunnitelma kyberturvallisuusopetusmateriaalista sekä lyhyt kuvaus sen luomisprosessista ja siitä, miten aiot hyödyntää opetusmateriaalia osana opetustasi tähän palautuslaatikkoon. Lisää myös palautettavan materiaalin loppuun lyhyt itsearviointi ja kerro vapaasti, mitä mieltä olit opintojakson toteutuksesta.

Palauta materiaali tähän palautuslaatikkoon yhtenä tiedostona tai verkkolinkkinä (tarkista, että jakoasetukset sallivat pääsyn tiedostoon). Huom! Tehtävänannon kohdat 6–9 eli opetusmateriaalin varsinainen toteutus, testaus, arviointi ja viimeistely on mahdollista tehdä myös opintojakson jälkeen.

OPETUSHALLITUS RAHOITTAA HANKETTA
jamk

Juttelutuokiot

Itsenäisen opiskelun lomassa sinun on mahdollista osallistua juttelutuokioihin, joihin voit siis nimensä mukaisesti tulla juttelemaan meidän opettajien ja muiden opiskelijoiden kanssa sotealan kyberturvallisuuteen liittyvistä teemoista, tämän opintojakson suorittamisesta tai oppimistehtävistä. Osallistuminen on vapaaehtoista ja hyvin vapaamuotoista. Tervetuloa mukaan!

Juttelutuokiot järjestetään Zoomissa.

OPETUSHALLITUS RAHOITTAA HANKETTA
jamk

Lähdemateriaalit

- Blek, T., & Solankallio-Vahteri, T. (2022). Information andcybersecurity competence of healthcare care personnel. Finnish Journal of EHealth and EWelfare, 14(4), 352–363.
- Cyberinsecurity in Healthcare. The cost and impact on patient safety and care. Proofpoint. 2023. Viitattu 7.1.2024. https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf
- CYBERDI-projekti (2021). Digihuijausten tunnistaminen ja niiltä suojautuminen – Opas yrityksille ja organisaatioille sekä Maija ja Matti Meikäläisille. Kansallista kyberosaamista kasvattamassa, CYBERDI-projekti 10/2018 – 12/2021
- Jerry-Egemba N. (2023). Safe and sound: Strengthening cybersecurity in healthcare throughrobust staff educational programs. Healthcare Management Forum, 37(1), 21–25.
- Kyberturvallisuus. Ohje sosiaali- ja terveysalan toimijoille. 2019. Sosiaali- ja terveysministeriö. Viitattu 7.1.2024. Kyberturvallisuus Ohje sosiaali- ja terveydenhuollon toimijoille (valtioneuvosto.fi)
- Paananen, R. 2021. Kyberturvallisuuden kehittämisohjelma. Liikenne- ja viestintäministeriön julkaisuja 2021: 7.
- Turvallisuuskomitea 2018. Kyberturvallisuuden sanasto. Sanastokeskus TSK 52.
- Valtioneuvosto 2022. Valtioneuvoston selonteko: Suomen digitaalinen kompassi. Valtioneuvoston julkaisuja 2022: 65.

OPETUSHALLITUS RAHOITTAA HANKETTA
jamk

Kyberturvallisuutta sote- ja hoiva-alan opettajille 2 op -verkkokoulutus

Koulutus on Opetushallituksen rahoittamaa opetustoimen henkilöstökoulutusta.

jamk

Koulutuksen materiaalit:

OPETUSHALLITUS RAHOITTAA HANKETTA

2. Sosiaali- ja terveysalaan kohdistuvat kyberturvallisuusuhat

Tiina Blek, lehtori,
Hyvinvointiyksikkö, Jyväskylän ammattikorkeakoulu

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Tapahtumakuvaus Yhdysvalloista

Marraskuu 2023

- Kyberhyökkäys vaikutti neljän osavaltion alueella toimiviin sairaaloihin
- Potilaita jouduttiin käännyttämään pois ensiavusta
- Suunniteltuja toimenpiteitä peruttiin
- Tietojärjestelmät pois käytöstä

Uutinen

Hakkerit iskivät jouluaattona kolmeen sairaalaan – kiristyshaittaohjelma teki ensiavun antamisesta mahdotonta

Marja Tienari 29.12.2023 13:45 | päivitetty 29.12.2023 13:45 KYBER KIRISTYSHAITTAOHJELMAT PALVELUNESTOHYÖKKÄYKSET TIETOTURVA HAITTAOHJELMAT HAKKERIT ENSIHOITO TERVEYSTEKNOLOGIA

Ransomware attack spreads chaos at a major hospital in Barcelona

Updated on: November 15, 2023 12:53 PM

Ulkomaat | **Yhdysvallat**

Kyberhyökkäys seisautti kiireellistä hoitoa neljän osavaltion alueella Yhdysvalloissa

Yhteensä 16:ta sairaalaa operoiva yritys kärsii tietoturvaan liittyvästä ongelmasta.

STT–AFP
5.8.2023 2:31

Hyvinvointialueet

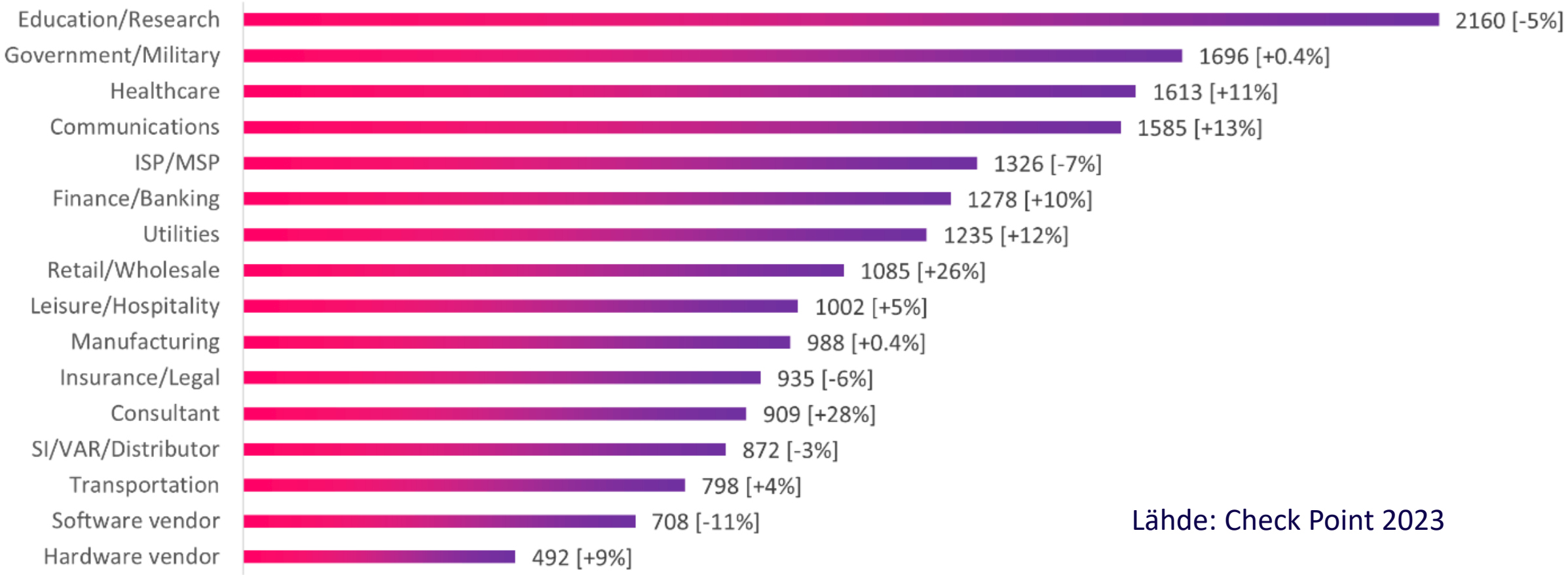
Tietomurto Tena-tuotteita kuljettavaan yritykseen – tuhansien asiakkaiden henkilötietoja vaarassa

https://yle.fi/

Uhkien yleisyys

- *Vuonna 2023 terveydenhuollon järjestelmiin kohdistui maailmanlaajuisesti keskimäärin 1613 kyberhyökkäystä viikossa.
  - Hyökkäysten määrässä noin 11 prosentin kasvu edellisvuoteen verrattuna.
  - Kiristyshaittaohjelman (ransomware) kohteeksi joutui keskimäärin noin joka 34. organisaatio (kaikki alat mukaan luettuna)
  - Terveydenhuoltoala oli toiseksi eniten alttiina näille hyökkäyksille. Joka 25. terveysalan organisaatio joutui kiristyshaittaohjelmahyökkäyksen kohteeksi.
    - Eniten kiristyshaittaohjelmahyökkäyksiä kohdistui hallinnon / armeijan järjestelmiin (joka 24. organisaatio)
- Hyökkäyksiä esiintyy kaikkialla maailmassa ja määrä lisääntyy vuosittain.

Global Average Weekly Cyber Attacks per Industy
(2023 vs. 2022)



Lähde: Check Point 2023

Miksi sote-järjestelmät houkuttavat verkkorikollisia?

- Terveysalan tietojärjestelmiä pidetään ”pehmeinä kohteina”
- Potilastietojärjestelmät ovat potilaiden hoidon kannalta elintärkeitä
- Potilastietojärjestelmien tiedot ovat sensitiivisiä ja salassa pidettäviä
- Potilastietojärjestelmän sisältämät tiedot ovat pimeillä markkinoilla arvokkaampaa kauppatavaraa, kuin esimerkiksi luottokorttitieto (tiedot eivät ole helposti muutettavia)
- Käytössä olevien laitteiden suuri määrä ja vanhentunut tekniikka
- Lääkinnälliset laitteet, joihin verkkorikolliset pääsevät helposti sisään
- Henkilökunta, jolla ei aina ole riittävää osaamista verkkoriskeistä
- Alalla vallitseva jatkuva kiire ja resurssipula
- Terveysalalla työskentelevien ominaispiirteet (luottamus, auttamisen halu)

jamk

Yleisimmät kyberuhat

- Terveydenhuollon järjestelmiin kohdistuvat yleisimmät kyberuhkat muodostuvat
  - tietomurroista (data breach)
  - tietojenkalastelusta (phishing, vhishing, smishing, spoofing)
  - kiristyshaittaohjelmista (ransomware) sekä
  - palvelunestohyökkäyksistä (denial of service, DoS)
  - lääkinnällisiin laitteisiin ja niiden kautta tapahtuvista hyökkäyksistä

- Tutustu näihin uhkiin myös Kyberhäiriöiden hallinta –käsikirjan avulla.

jamk

Lähteet

Check Point. 2023. Viitattu 4.1.2024. A Continuing Cyber-Storm with Increasing Ransomware Threats - Check Point Blog.

Kyberhäiriöiden hallinta. Käsikirja terveydenhuollon toimijoille. Viitattu 5.1.2024. kyberhairioiden-hallinta-kasikirja-terveydenhuollon-toimijoille.pdf (jyvsectec.fi)

Kyberturvallisuus. Ohje sosiaali- ja terveydenhuollon toimijoille. Viitattu 5.1.2024. Kyberturvallisuus Ohje sosiaali- ja terveydenhuollon toimijoille (valtioneuvosto.fi)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

3. Kyberhyökkäysten vaikutukset potilasturvallisuuteen ja henkilöstöön

Tiina Blek, lehtori, Hyvinvointiyksikkö, Jyväskylän ammattikorkeakoulu

OPETUSHALLITUS RAHOITTAA HANKETTA

jamk

Kyberhyökkäykset – vain isojen organisaatioiden uhka?

- Kyberhyökkäyksiä tapahtuu sekä pieniin, keskisuuriin että isoihin organisaatioihin.
- Verkkohyökkäyksiä tapahtuu valikoimattomasti ja ne vaikuttavat haitallisesti potilasturvallisuuteen ja henkilöstön toimintaan, riippumatta organisaation koosta, erikoisalasta tai muusta tekijästä.
- Kyberhyökkäysten vaikutukset koskevat organisaation kaikkien henkilöstöryhmien toimintaan (johtajat, it-henkilöstö, kliininen henkilöstö, toimistopalvelut jne.)

jamk

Kustannukset maailmanlaajuisesti

- Vuonna 2023 terveydenhuoltoon kohdistuneen tietomurron keskimääräinen kustannus oli 10,93 miljoonaa dollaria per murto —
  - Kustannus on lähes kaksinkertainen verrattuna finanssialaan, joka sijoittui toiseksi keskimääräisellä kustannuksellaan 5,9 miljoonaa dollaria.
- Lahden kaupungin järjestelmiin (2019) tapahtuneen hyökkäyksen kustannukset arviolta noin miljoona euroa.
- Taloudelliset vaikutukset sote-organisaatioiden toimintaan merkittävät

jamk

Terveydenhuollon toimintaympäristöstä raportoituja hyökkäyksiä

- Lääkintälaitteisiin kohdistuneita ja niiden kautta tapahtuneita hyökkäyksiä on toteutettu muun muassa verikaasuanalysaattoreiden sekä röntgen ja MRI-laitteiden kautta
- Potilaan itsensä hakkeroima PCA-(kipu)pumppu, jolla lisäsi itselleen määrättyä opioidiannosta → johti yliannostukseen (Itävalta)
- Potilasmonitorien sulkeminen (Etelä-Amerikka)
- Lääkepumppujen toiminnan estäminen (USA)

Vaikutukset potilasturvallisuuteen

- Hoidon viivästyminen osastojen ja sairaaloiden sulkemisen vuoksi
- Tutkimusten / kuvantamisen viivästymisistä aiheutuvat seuraamukset
- Lääkintälaitteiden häiriöiden aiheuttamat vaikutukset
- Henkilötietojen varastamisesta aiheutuvat vahingot

Vaikutukset henkilöstön toimintaan

Vaikutukset riippuvat hyökkäyksen muodosta (esim. kiristyshaittaohjelma vs. tietomurto)

- Potilastiedot eivät ole käytettävissä
  - Hoito-ohjeet
  - Potilaan sairaushistoria / terveystiedot
  - Lääkehoidon tiedot
  - Laboratorio- ja kuvantamisen tulokset
- Lääkinnällisten laitteiden käyttö rajoitettua / ei käytettävissä
- Sähköposti ei käytettävissä
- Verkkoyhteydet ei käytettävissä

jamk

Lähteet

- Healthcare pays the highest price of any sector for cyberattacks — that's why cyber resilience is key. 2024. World Economic Forum. Viitattu 14.2.2024. https://www.weforum.org/agenda/2024/02/healthcare-pays-the-highest-price-of-any-sector-for-cyberattacks-that-why-cyber-resilience-is-key/.
- Moore, G., Khurshid, Z., McDonnell, T., Rogers, L. & Healy, O. 2023. A resilient workforce: patient safety and the workforce response to a cyber-attack on the ICT systems of the national health service in Ireland. BMC Health Services Research (2023) 23:1112. Viitattu 16.2.2024. https://doi.org/10.1186/s12913-023-10076-8.
- O'Brien N., Ghafur S. & Durkin M. Cybersecurity in health is an urgent patient safety concern: We can learn from existing patient safety improvement strategies to address it. Journal of Patient Safety and Risk Management. 2021;26(1):5-10. Viitattu 26.1.2024. https://doi.org/10.1177/2516043520975926.

jamk

2024

Tiina Blek

5. Sote-alan ammattilaisten kyberturvallisuus-osaamistarpeet

Johanna Niskakangas, lehtori
Tiina Blek, lehtori
Hyvinvointiyksikkö, Jyväskylän ammattikorkeakoulu

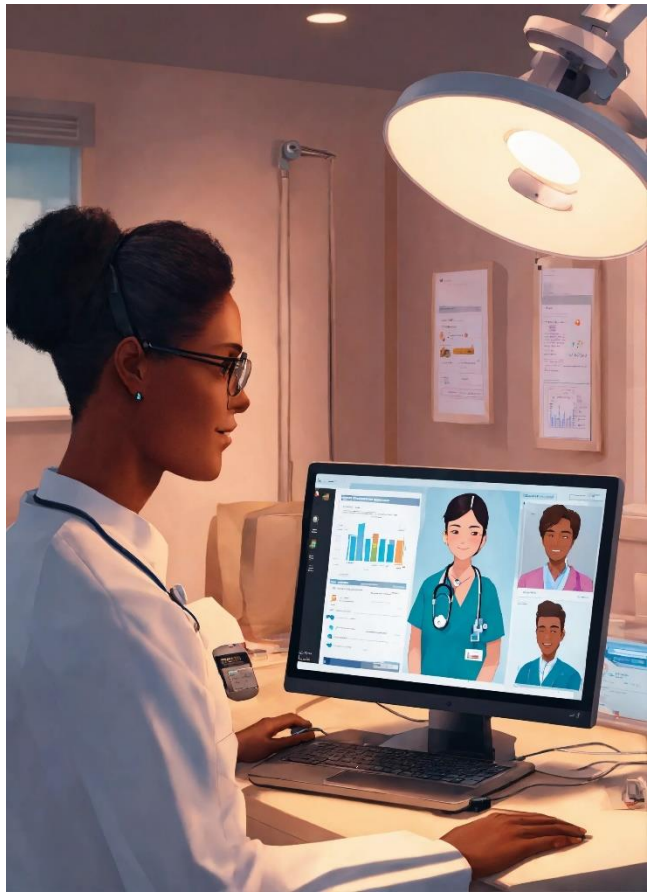
jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

OPETUSHALLITUS RAHOITTAA HANKETTA

Miksi kyberosaamista tarvitaan?

Ei ainoastaan IT:n ongelma

- Kyberturvallisuusosaaminen on osa koko sote-henkilöstön osaamistarvetta (Cartwright 2023; ENISA 2023)
- Teknisillä keinoilla voidaan suojautua kyberrikoksia vastaan, mutta valistuneen henkilöstön ja vahvan tietoturvakulttuurin puuttuminen jättävät organisaation suojauksen vajaaksi (Kamerer & McDermott 2020) → Ihmispalomuuri!
- Kyberturvallisuudessa kyse muustakin kuin teknologiasta (Jerry-Egemba 2023) → Kyberturvallisuusosaamisessa kyse muustakin kuin teknologisesta osaamisesta
- Kyberriskien ymmärtäminen ja omien toimien vaikutusten tunnistaminen kasvattavat koko organisaation kyberturvallisuutta → osaamista lisättävä (Rajamäki ym. 2023)

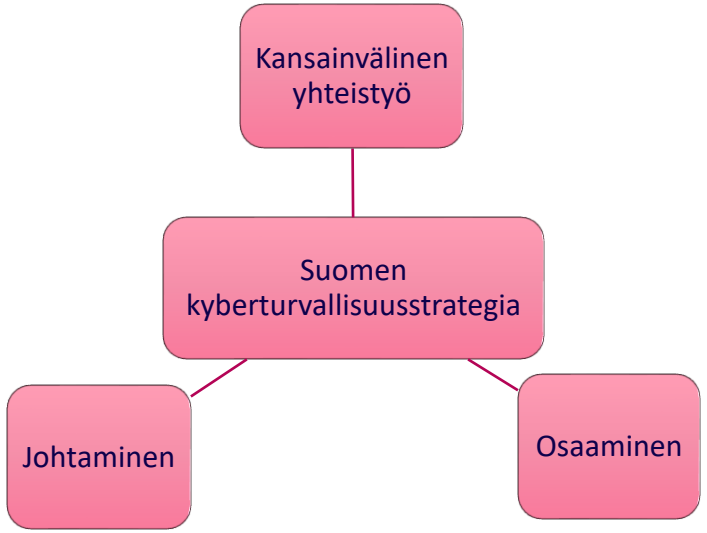


jamk

Kaikilla tulisi olla kyberturvallisuusosaamista!

Kyberturvallisuuden osaamisen kehittäminen yksi keskeisistä Suomen kyberturvallisuusstrategian tavoitteista (Turvallisuuskomitea 2019)

- Kansallinen kyberturvallisuuden osaaminen varmistetaan:
  - Tunnistamalla osaamistarve sekä vahvistamalla koulutusta ja tutkimusta
  - Viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä (jokainen voi osaltaan vaikuttaa yhteiseen kyberturvallisuuteemme)
  - Varmistamalla, että jokaisella on riittävät valmiudet toimia turvallisesti digitaalisessa toimintaympäristössä
- **”Jokainen yksilö on siten tärkeä kyberturvallisuustoimija**, joka omilla arjen kyberturvallisuutta parantavilla teoilla voi vaikuttaa omaan ja muiden kyberturvallisuuteen.” (Turvallisuuskomitea 2019)



jamk

Kyberosaaminen sotessa

- Ihmiset ja heidän toimintansa nähdään suurimpana uhkana kyberturvallisuuden toteutumiselle sote-alan organisaatioissa (Kioskli ym. 2023; Rajamäki ym. 2023)
- Terveysalan henkilöstön keskuudessa vielä heikosti tietoa… (Rajamäki ym. 2023)
  - …kyberturvallisuusuhista ja -riskeistä
  - …oman toiminnan vaikutuksista organisaation kyberturvallisuuteen
- Alalla selkeä täydennyskoulutustarve kyberturvallisuuteen liittyen (ks. Blek & Solankallio-Vahteri 2022; Haukilehto 2024)

jamk

Kyberosaaminen sotessa

- Kyselytutkimus Suomessa kahdessa sairaanhoitopiirissä ja yhdessä perusterveydenhuollon yksikössä (n = 194 hoitotyön tehtävissä olevaa henkilöä) (Blek & Solankallio-Vahteri 2022)

  87 % lukenut organisaation tietoturvaohjeet
  9 % antaisi salasanan puhelimitse tietohallinnolle
  14 % antaisi salasanan puhelimitse viranomaiselle
  8 % oli sitä mieltä, että opiskelija voi käyttää ohjaajansa käyttäjätunnuksia
  9 % käyttänyt kollegan käyttäjätunnusta
  74 % arvioi tieto- ja kyberturvallisuustaitonsa riittäviksi tehtäviensä hoitamiseen (19 % ”täysin samaa mieltä”)
  83 % tietää, miten toimia tietojärjestelmähäiriön sattuessa
  Myös informaatiovaikuttamisen ja GDPR:n osalta selkeä tiedon vajaus

- Kyselytutkimus, jossa mukana useita terveydenhuollon organisaatioita ja heidän työntekijöitään (n = 881) (Haukilehto 2024)

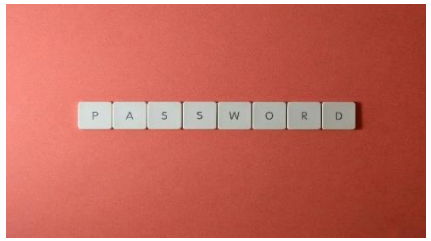
  38 % ei ollut lukenut organisaation tietoturvaohjeita
  77 % oli riittävästi tietoa tieto- ja kyberturvallisuudesta työnsä kannalta

jamk

Koulutetaanko kyberturvallisuutta riittävästi?

- Kyselytutkimus Suomessa kahdessa sairaanhoitopiirissä ja yhdessä perusterveydenhuollon yksikössä, n = 383 (sote-henkilöstöä) (Blek ym. 2023)
  - 38 % oli saanut koulutusta haittaohjelmien torjumista vastaan
  - 44 % koki, että nykyinen tieto- ja kyberturvallisuuskoulutus oli riittävällä tasolla
  - 84 % osoitti kiinnostusta saada lisäkoulutusta tietoturvallisuudesta, tietosuojasta ja kyberturvallisuudesta
- Kyselytutkimus, jossa mukana useita terveydenhuollon organisaatioita ja heidän työntekijöitään (n = 881) (Haukilehto 2024)
  - 56 % ei ollut osallistunut mihinkään kyberturvallisuuteen liittyvään koulutukseen tai luennolle
    - Vain muutamia vastauksia, että ei tarvetta lisätiedolle aiheesta

Sote-ammattilaisten tärkeimmät osaamiset



Oma kyberturvallinen tapa toimia

Kyberhäiriöiden vaikutusten tunnistaminen

Laitteisiin ja välineisiin liittyvien kyberturvallisuusuhkien tunnistaminen

Kyberhäiriötilanteessa toimiminen

Lähde: Isännäinen & Tulkki 2022; Rajamäki ym. 2023

jamk

Lähteet

- Blek, T., Mäkelä, J. & Solankallio-Vahteri, T. 2023. Assessing information and cybersecurity training needs among social and healthcare professionals. Finnish society of telemedicine and eHealth (FSTeH) publication 1/2023.
- Blek, T. & Solankallio-Vahteri, T. 2022. Terveydenhuollon hoitohenkilöstön tieto- ja kyberturvallisuusosaaminen. FinJeHeW 14 (4): 352–363
- Cartwright, A. J. (2023). The elephant in the room: Cybersecurity in healthcare. Journal of Monitoring and computing, 37, 1123–1132. Coventry, L., Branley-Bell, D., Sillence, E., Magalini, S., Mari, P., Magkanaraki, A. & Anastasopoulou, K. 2020. Cyber-risk in Healthcare: Exploring facilitators and barriers to secure behaviour. HCI for Cybersecurity, Privacy and Trust.
- European Union Agency for cybersecurity (ENISA) 2023. ENISA threat landscape: health sector (January 2021 to March 2023). https://www.enisa.europa.eu/publications/health-threat-landscape
- Haukilehto, T. 2024. Cybersecurity management in healthcare. Policies, awareness and incident reporting. Acta Wasaensia 532.
- Isännäinen, A. & Tulkki, S. 2022. Kyberturvallisuus terveydenhuollossa. Mitä sairaanhoitajan tulee tietää ja osata?
- Kamerer, J. & McDermott, D. (2020). Cybersecurity: nurses on the front line of prevention and education. Journal of nursing regulation, 10(4), 48–53.
- Martin, G., Martin, P., Hankin, C., Darzi, A. & Kinross, J. 2017. Cybersecurity and healtcare: how safe are we? BMJ 358: j3179. doi: 10.1136/bmj.j3179
- 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.
- Turvallisuuskomitea. (2019). Suomen kyberturvallisuusstrategia 2019. Valtioneuvoston periaatepäätös 3.10.2019. Viitattu 26.5.2024. Saatavilla: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf

jamk

jamk