HAMK
Hämeen ammatti-
korkeakoulu

Kyberturvallisuus hoitotyössä

Sairaanhoitajaopiskelijoiden tietoturvaosaamisen vahvistaminen

Ammattikorkeakoulun opinnäytetyö
Sähkö- ja automaatiotekniikka, insinööri (AMK)
Syksy 2024
Juuso Mäntymäki

HAMK
Hämeen ammatti-
korkeakoulu

Sähkö- ja automaatiotekniikka, insinööri
Tekijä Juuso Mäntymäki
Työn nimi Kyberturvallisuus hoitotyössä
Ohjaaja Juha Sarkula

Tiivistelmä
Vuosi 2024

Tämän opinnäytetyön tavoitteena oli lisätä sairaanhoitajaopiskelijoiden kyberturvallisuustietoisuutta ja kehittää heidän valmiuksiaan soveltaa kyberturvallisuuden periaatteita hoitotyön arjessa. Tutkimuksen tarkoituksena oli kartoittaa terveydenhuollon hoitohenkilökunnan tietosuoja- ja kyberturvallisuustietoisuutta sekä hyödyntää saatuja tietoja kohdennetun opetusmateriaalin kehittämisessä. Lisäksi tutkimuksessa selvitettiin, miten opetusmateriaali ja siihen liittyvä luento vaikuttivat sairaanhoitajaopiskelijoiden kyberturvallisuustietämykseen. Työn toimeksiantajana toimi Hämeen ammattikorkeakoulu.

Opinnäytetyön tutkimusmenetelminä käytettiin teoreettista viitekehystä, joka perustui ajankohtaisiin lähteisiin kyberturvallisuudesta erityisesti terveydenhuollon kontekstissa. Näiden pohjalta laadittiin opetusmateriaali, joka esiteltiin luennolla sairaanhoitajaopiskelijoille. Luentoon osallistuneilta opiskelijoilta kerättiin anonyymiä palautetta, jonka avulla arvioitiin opetusmateriaalin ja luennon onnistumista.

Tulokset osoittivat, että opiskelijat kokivat luennon selkeäksi ja hyödylliseksi, ja erityisesti käytännön esimerkit tukivat oppimista. Palautteen perusteella opiskelijat kokivat ymmärtävänsä kyberturvallisuuden merkityksen hoitotyössä aiempaa paremmin ja arvioivat, että heidän tietämyksensä oli parantunut merkittävästi koulutuksen jälkeen.

Opinnäytetyö vahvisti, että sairaanhoitajaopiskelijoille suunnattu kyberturvallisuuskoulutus on sekä tarpeellista että vaikuttavaa. Se edistää opiskelijoiden valmiuksia suojata potilastietoja, tunnistaa kyberuhkia ja toimia tietoturvallisesti. Tulokset korostavat, että kyberturvallisuus tulisi sisällyttää osaksi sairaanhoitajakoulutusta, jotta tulevat ammattilaiset voivat vastata digitalisoituvan terveydenhuollon vaatimuksiin ja ylläpitää potilasturvallisuutta.

Avainsanat hoitotyö, kyberturvallisuus, tietoturva

Sivut 39 sivua ja liitteitä 16 sivua

HAMK
Hämeen ammatti-
korkeakoulu

Electrical and automation engineering
Author Juuso Mäntymäki
Subject Cyber security in nursing
Supervisors Juha Sarkula

Abstract
Year 2024

The aim of this thesis was to enhance nursing students' awareness of cybersecurity principles and develop their ability to apply these principles in everyday nursing practice. The purpose of the study was to assess the awareness of data protection and cybersecurity among healthcare personnel and use these findings to create targeted teaching materials for nursing students. Furthermore, the study investigated how the teaching material and an accompanying lecture influenced the nursing students' knowledge of cybersecurity. The thesis was commissioned by Häme University of Applied Sciences.

The research methods included a theoretical framework based on up-to-date sources on cybersecurity in the healthcare context. This framework was used to design teaching materials, which were presented during a lecture to nursing students. Anonymous feedback was collected from the participants to evaluate the effectiveness of the teaching materials and the lecture.

The results showed that students found the lecture clear and useful, with practical examples particularly supporting their learning. Feedback indicated that the students gained a better understanding of the significance of cybersecurity in nursing and reported a considerable improvement in their knowledge following the training.

This thesis confirmed that cybersecurity training for nursing students is both necessary and impactful. It enhances students’ ability to protect patient information, recognize cyber threats, and act in a secure manner. The findings emphasize that cybersecurity should be incorporated into nursing education to prepare future professionals to meet the demands of an increasingly digitalized healthcare environment and maintain patient safety.

Keywords nursing, cyber security, information security
Pages 39 pages and appendices 16 pages

Sisällys

1 Johdanto 1

1.1 Tutkimuksen tausta ja merkitys 1

1.2 Tutkimuksen tavoitteet ja tutkimuskysymykset 2

1.3 Teoreettisen viitekehityksen lähdeaineisto 3

2 Teoreettinen viitekehys 4

2.1 Kyberturvallisuuden peruskäsitteet ja termistö 4

2.2 Johdanto kyberturvallisuuteen hoitotyössä 5

2.2.1 Kyberhyökkäykset terveydenhuollossa 5

2.2.2 Sairaanhoitajan rooli kyberturvallisuudessa 8

2.3 Kyberhyökkäysmetodeja terveydenhuollossa 9

2.3.1 Tietojen kalastelu 9

2.3.2 Kohdistettu tietojen kalastelu 12

2.3.3 Kiristysohjelma 14

2.3.4 Kyberuhat tulevaisuudessa 16

2.4 Käytännön keinot suojautua hoitotyössä 17

2.4.1 Salasanat 17

2.4.2 Sähköpostin turvallinen käyttäminen 18

2.4.3 Työaseman käyttäminen 19

2.4.4 Varmuuskopiointi 20

2.4.5 Kaksivaiheinen tunnistautuminen varmennekortilla 21

2.5 Kyberuhkien ilmoittaminen hoitotyössä 22

2.6 Potilastietojen käsittely ja suojaaminen 23

2.6.1 Potilastietojen luovuttaminen 23

2.6.2 Potilastietojen kirjaaminen 24

3 Opinnäytetyön toteutusmenetelmä 26

3.1.1 Teoreettisen viitekehyksen aineiston kerääminen ja rajaus 26

3.1.2 Opetusmateriaalin kehittäminen 27

3.1.3 Opetusmateriaalin testaaminen ja palaute 27

3.1.4 Opetusmateriaalin ulkoasu 27

4 Tulokset 32

4.1 Palautekyselyn tulokset 32

4.2 Tutkimuksen tulokset 33

5 Pohdinta 36

Lähteet 39

Kuvat, taulukot ja kaavat

Kuva 1. Yli 500 tietueen terveydenhuollon tietomurrot (2009–2004) 6

Kuva 2. Tietojenkalastelu tekstiviestit..... 11

Kuva 3. Turvapostikalasteluviesti (Traficom, 2023) 13

Kuva 4. Microsoft-teemainen kalastelusivusto (Traficom, 2023)..... 13

Kuva 5. Kiristyshaittaohjelma WannaCry (BBC, 2017) 14

Kuva 6. Järjestelmien salasanataulukko (Hive systems, 2024) 18

Kuva 7. Tehtäväpalkin kuvake VPN-yhteydestä..... 20

Kuva 9. Tekoälyllä generoitu kuva sairaalasta 28

Kuva 10. Tekoälyllä generoitu kuva hoitajista 28

Kuva 11. Tekoälyllä generoitu kuva sairaalan sisätiloista..... 29

Kuva 12. Tekoälyllä generoitu kuva hoitajasta työntämässä sänkyä 29

Kuva 13. Tekoälyllä generoitu kuva lukosta kyberturvallisuudessa 30

Kuva 14. Tekoälyn generoima kuva sairaalasta..... 30

Kuva 15. Tekoälyllä generoitu kuva työpöydästä 31

Kuva 16. Tekoälyllä generoitu kuva Sote ammattikortista 31

Liitteet

Liite 1. PowerPoint esitys kyberturvallisuus hoitotyössä

Liite 2. Webropol palautekyselylomake

1 Johdanto

1.1 Tutkimuksen tausta ja merkitys

Terveydenhuollon kyberturvallisuus on kriittinen aihe, sillä se suojaa potilastietoja ja terveydenhuollon infrastruktuuria. Terveydenhuollossa käsitellään erittäin arkaluontoisia tietoja, ja niiden suojaaminen on elintärkeää potilaiden yksityisyyden ja turvallisuuden varmistamiseksi. Kyberturvallisuuden puutteet voivat johtaa vakaviin seurauksiin, kuten potilastietojen vuotamiseen, palvelun keskeytymiseen tai jopa terveydenhuollon järjestelmien toimintakatkoksiin, jotka voivat vaikuttaa potilaiden hoitoon ja turvallisuuteen.

Sairaanhoitajaopiskelijat ovat tulevaisuuden ammattilaisia, jotka työskentelevät päivittäin potilastietojen kanssa. Heidän kouluttamisensa kyberturvallisuuden perusteista on tärkeää, jotta he pystyvät suojaamaan potilastiedot ja varmistamaan tietoturvan hoitotyössä. Tietoisuuden ja käytännön valmiuksien kehittäminen jo opiskeluvaiheessa voi vähentää merkittävästi tietoturvauhkiin liittyviä riskejä ja parantaa koko terveydenhuoltojärjestelmän resilienssiä.

Tämä opinnäytetyö on merkittävä, sillä se paikkaa HAMKin sairaanhoitajaopiskelijoiden koulutuksessa olevan aukon kyberturvallisuuden osalta hoitotyössä. Vaikka opiskelijat saavat usein kyberturvallisuuskoulutusta tai -ohjeistusta vasta työharjoittelussa tai työsuhteen alkaessa, olisi erittäin tärkeää, että koulu tarjoaisi jo opiskeluvaiheessa perustason koulutusta kyberturvallisuudesta ja tietosuojasta ennen työelämään siirtymistä. Tämä varmistaisi, että opiskelijat omaksuvat keskeiset tietoturvakäytännöt ajoissa ja ovat paremmin valmistautuneita ammatillisiin vastuisiin heti uran alkuvaiheessa. Työpaikoilla on lopullinen vastuu kattavan kyberturvallisuuskoulutuksen järjestämisestä. Varhainen ohjeistus koulun puolelta valmentaisi opiskelijoita paremmin tuleviin tehtäviinsä terveydenhuollon ammattilaisina.

Opinnäytetyön toimeksiantajana toimii Hämeen ammattikorkeakoulu, ja sitä käytetään sairaanhoitajaopiskelijoiden kyberturvallisuuskoulutuksessa. Työn tutkimus tuo merkittävän panoksen hoitotyön kyberturvallisuuskoulutuksen kehittämiseen, arvioiden opetusmateriaalin vaikuttavuutta. Sen pohjalta voidaan kehittää koulutusmenetelmiä ja -materiaaleja, jotka vastaavat tehokkaasti opiskelijoiden tarpeisiin.

1.2 Tutkimuksen tavoitteet ja tutkimuskysymykset

Tutkimuksen tavoitteena on kartoittaa terveydenhuollon hoitohenkilökunnan tietosuoja- ja kyberturvallisuustietoisuutta sekä selvittää, millaisia kyberuhkia hoitohenkilökunta kohtaa hoitotyön arjessa. Tavoitteena on ymmärtää, kuinka hyvin hoitohenkilökunta tuntee tietoturvaan ja kyberturvallisuuteen liittyvät periaatteet, sekä arvioida heidän valmiuksiaan suojata potilastietoja ja reagoida kyberturvallisuusuhkiin. Näiden tulosten perusteella kehitetään opetusmateriaali, jonka avulla sairaanhoitajaopiskelijat voivat paremmin valmistautua kohtaamaan työelämän tietoturvahaasteet.

Opetusmateriaalin ja koulutuksen tarkoituksena on parantaa opiskelijoiden kyberturvallisuustietoisuutta ja auttaa heitä ymmärtämään kyberturvallisuuden merkitys terveydenhuollossa. Tutkimuksessa arvioidaan opetusmateriaalin ja koulutuksen vaikutusta opiskelijoiden valmiuksiin soveltaa kyberturvallisuuden periaatteita käytännön hoitotyössä. Tavoitteena on kehittää koulutussisältöä, joka vastaa hoitotyön vaatimuksiin ja auttaa suojaamaan potilastietoja.

Tutkimuskysymykset:

Miten hyvin hoitohenkilökunta tuntee tietosuojaan ja kyberturvallisuuteen liittyvät periaatteet?

Millaisia kyberuhkia hoitohenkilökunta kohtaa päivittäisessä työssään?

Kuinka hyvin sairaanhoitajaopiskelijat ymmärtävät kyberturvallisuuden periaatteet ja niiden soveltamisen hoitotyössä koulutuksen jälkeen?

Miten tehokasta opetusmateriaali on opiskelijoiden kyberturvallisuusosaamisen kehittämisessä?

Millaisia vaikutuksia koulutuksella on opiskelijoiden tietoisuuteen kyberturvallisuudesta ja sen merkityksestä hoitotyössä?

1.3 Teoreettisen viitekehityksen lähdeaineisto

Teoreettisen viitekehyksen lähdeaineisto koostuu valikoimasta ajankohtaisia ja relevantteja lähteitä vuosien 2017-2024 väliltä, sillä terveydenhuollon kyberturvallisuudessa on rajallisesti nykypäiväistä tietoa ennen vuotta 2017. Tämä aikarajaus varmistaa, että tutkimus sekä opetusmateriaali perustuvat tuoreisiin ja relevantteihin tietoihin.

Lähdeaineisto käsittelee kyberturvallisuutta hoitotyössä. Se sisältää tutkimusartikkeleita ja tieteellisiä julkaisuja, lakitekstejä ja standardeja, raportteja sekä tilastoja. Lisäksi opetusmateriaalin luomisessa hyödynnetään aikaisemmin mainittujen lisäksi kyberturvallisuuden verkkokoulutuksia ja opetusvideoita.

Lähdeaineiston etsintäprosessissa hyödynnetään monipuolisesti erilaisia hakukoneita ja tietokantoja. Google ja Google Scholar -haut ovat keskeisessä roolissa. Hakusanoja syötetään sekä suomen että englannin kielellä, jotta saadaan mahdollisimman laaja ja kattava aineisto. Suomeksi käytettyjä hakusanoja ovat muun muassa "kiristyshaittaohjelma", "kyberturvallisuus hoitotyössä", "kyberturvallisuus terveydenhuollossa", "kyberturvallisuus tilasto", "Potilas- ja asiakastietojen ja henkilötietojen käsittely", "tietojen kalastelu", "tietoturva". Englanniksi käytettyjä hakusanoja ovat esimerkiksi "cyber security in nursing", "cyber security statistics", "cybersecurity in healthcare", "Information security", "patient and document processing", "Phishing", "ransomware".

2 Teoreettinen viitekehys

2.1 Kyberturvallisuuden peruskäsitteet ja termistö

Kyberturvallisuus tarkoittaa keinoja ja toimia, joilla suojataan laitteita, tietoja ja verkkoja hyökkäyksiltä ja muilta vaaroilta. Se on erityisen tärkeää sähköisissä toiminnoissa ja kriittisissä infrastruktuureissa, kuten terveydenhuollossa, maksuliikenteessä ja energiaverkoissa. Kyberturvallisuus suojaa verkkojen käyttäjiä sekä valtioiden että yksityisten tahojen hyökkäyksiltä, ja se on keskeinen osa myös tietoturvaa, mutta keskittyy erityisesti verkko- ja digitaaliympäristöjen suojaamiseen. (F-Secure, 2024c)

Takaovi on ohjelmistoon tahallaan tai vahingossa jätetty piilotettu reitti, jonka kautta järjestelmään voi päästä ohi normaalien turvamekanismien. Hyökkääjät voivat käyttää takaovia järjestelmän hallintaan, tietojen varastamiseen tai lisähyökkäysten valmisteluun. (Traficom, 2020b)

Tietomurto tarkoittaa luvatonta pääsyä tietojärjestelmiin, palveluihin tai sovelluksiin. Hyökkääjä voi käyttää varastettuja tunnuksia tai murtautua suoraan järjestelmään, usein taloudellisen hyödyn tavoittelussa. Tietoja voidaan varastaa ja myydä eteenpäin, tai murrettua ympäristöä voidaan käyttää haitallisen sisällön jakeluun tai lamauttaa se kiristysohjelmilla. Tietomurto voi aiheuttaa organisaatiolle taloudellisia ja mainehaittoja sekä keskeyttää toiminnan pitkiksikin ajoiksi. (Traficom, 2022b)

Tietoturva tarkoittaa arkaluonteisten tietojen suojaamista niiden elinkaaren ajan luvattomalta käytöltä, menettämiseltä tai väärinkäytöltä. Se kattaa toimenpiteet, joilla hallitaan käyttäjien pääsyä tietoihin ja varmistetaan tietojen turvallisuus erilaisissa tilanteissa, kuten järjestelmävioissa tai tietomurroissa. Tietoturvaan kuuluu käyttöoikeuksien hallinta, käyttäjän todennus, salaus, varmuuskopiot, tietojen hävittäminen sekä sisäisten riskien hallinta. Näillä toimenpiteillä varmistetaan esimerkiksi henkilökohtaisten, taloudellisten ja terveystietojen suojaus sekä säädösten noudattaminen. (Microsoft, 2024d)

Tietue (healthcare record) on kokoelma tietoja, jotka sisältävät potilaan henkilö- ja terveystiedot, kuten diagnoosit, hoitohistorian, laboratoriotulokset ja muita hoitoon liittyviä tietoja. Nämä tietueet ovat keskeisiä potilaan hoidon suunnittelussa ja toteutuksessa, ja ne tallennetaan usein sähköisiin potilastietojärjestelmiin. Tietueiden suojaaminen on tärkeää, koska tietomurrot voivat paljastaa arkaluonteisia potilastietoja. (Alder, 2024)

Tietoturvaloukkaus tarkoittaa järjestelmän luvattomasta käytöstä johtuvaa tietojen vaarantumista. Hyökkäys voidaan havaita useilla tavoilla, kuten järjestelmän odottamattomalla toiminnalla, tietoturvaohjelmiston hälytyksillä, tai ilmoituksilla ulkopuolisilta tahoilta. Joskus hyökkäys paljastuu vasta, kun vakava haavoittuvuus korjataan tai hyökkääjä yrittää kiristää varastetuilla tiedoilla. Loukkauksen tapahduttua on tärkeää ilmoittaa siitä Kyberturvallisuuskeskukselle, joka tarjoaa tukea vahinkojen hallintaan ja auttaa palautumisprosessissa. (Traficom, 2022b)

SOC (Security Operations Center) on tietoturvakeskus, joka valvoo organisaation tietoverkkoa, havaitsee uhkia ja reagoi niihin suojatakseen järjestelmiä kyberhyökkäyksiltä (IBM Technology, 2023).

2.2 Johdanto kyberturvallisuuteen hoitotyössä

2.2.1 Kyberhyökkäykset terveydenhuollossa

Kyberturvallisuus terveydenhuollossa on yhä kasvava huolenaihe, koska alan digitalisoituminen on tehnyt potilastiedoista arvokkaan kohteen kyberrikollisille. Terveydenhuollon toimijat, kuten sairaalat ja pienet terveyskeskukset, käsittelevät erittäin arkaluonteista tietoa, kuten potilaiden henkilötietoja ja terveystietoja. Jos nämä tiedot päätyvät vääriin käsiin, seuraukset voivat olla vakavia: identiteettivarkauksia, väärinkäytöksiä tai potilasturvallisuuden vaarantumista. Kyberhyökkäykset voivat myös häiritä terveydenhuollon toimintoja, aiheuttaen käyttökatkoksia potilastietojärjestelmiin, mikä hidastaa hoitoa ja lisää terveysriskejä. Hyökkäyksen kohteena oleminen voi lisäksi vaarantaa organisaation maineen, mikä johtaa taloudellisiin tappioihin ja luottamuksen menettämiseen potilaiden ja sidosryhmien keskuudessa. (Bowcut, 2023)

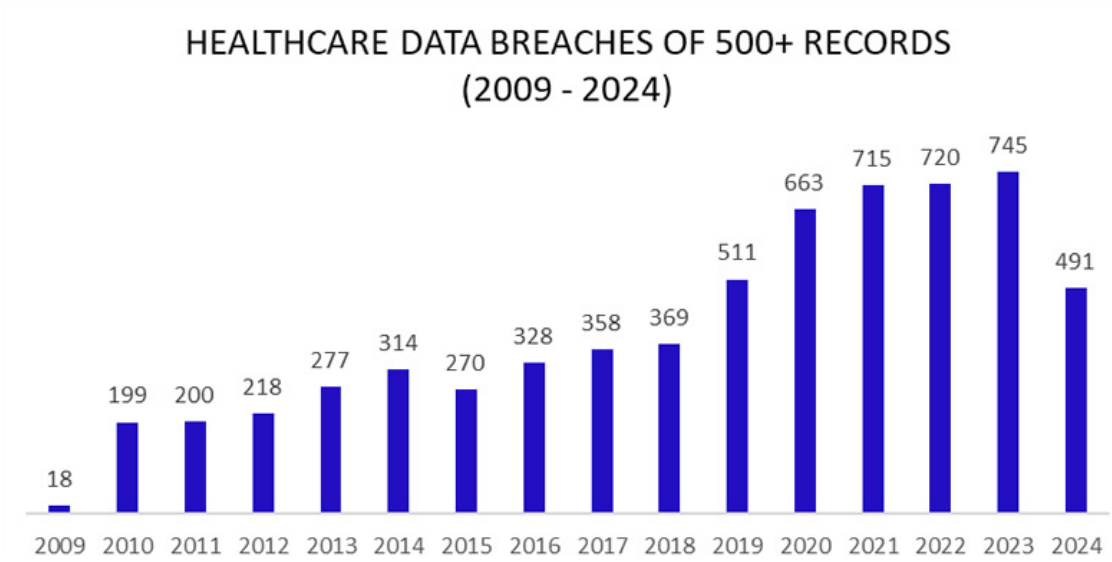
Erityisen haavoittuvia ovat pienet terveydenhuollon toimijat, joilla ei usein ole samanlaisia resursseja tai asiantuntemusta kyberturvallisuuden varmistamiseksi kuin suuremmilla organisaatioilla. Haasteita aiheuttavat vanhentuneet tietojärjestelmät, heikot tietoturvakäytännöt ja usein riittämätön henkilöstön koulutus kyberuhkien tunnistamisessa ja torjunnassa. Tietoturvaongelmat voivat myös liittyä fyysiseen laitteistoturvallisuuteen, kuten suojaamattomiin työasemiin tai puutteelliseen pääsynvalvontaan. (Bowcut, 2023)

Etätyön lisääntyminen terveydenhuollossa on tuonut mukanaan merkittäviä tietoturvahaasteita, sillä nopea siirtyminen digitaalisiin palveluihin on saattanut aiheuttaa

tietoturva-aukkoja etäyhteyksissä ja pilvipalveluissa. Omien laitteiden käyttö työtehtävissä lisää riskejä, kun työntekijät asentavat sovelluksia ja käsittelevät potilastietoja henkilökohtaisilla sähköpostitileillä tai kotiverkoissa, jotka eivät välttämättä ole yhtä turvallisia kuin organisaation tarjoamat verkot. Lisäksi salassa pidettävien tietojen tulostaminen kotona ilman riittävää suojaa ja kirjautumistietojen huoleton jakaminen voivat altistaa tietovuodoille. Tämän vuoksi etätyössä on tärkeää kiinnittää erityistä huomiota tietoturvatoimiin potilastietojen ja muiden arkaluonteisten tietojen suojaamiseksi. (Vertainen ym., 2024)

Terveydenhuollon tietomurrot ovat lisääntyneet huomattavasti viimeisen vuosikymmenen aikana. Vuodesta 2009 lähtien Yhdysvaltain terveysministeriön toimisto (Office for Civil Rights, OCR) on kerännyt ja julkaissut tietoja terveydenhuollon tietomurroista, joissa on vuotanut vähintään 500 tietuetta (kuva 1). Yhteensä 5 887 suurta tietomurtoa on raportoitu vuoteen 2023 mennessä, mikä on johtanut lähes 520 miljoonan terveydenhuollon tietueen paljastumiseen tai luvattomaan luovuttamiseen. Tämä määrä on yli 1,5 kertaa Yhdysvaltojen väkiluku. Erityisesti viime vuosina tietomurtojen määrä on ollut kasvussa. Vuonna 2023 raportoitiin keskimäärin 1,99 tietomurtoa päivässä, ja näissä murroissa keskimäärin 364 571 terveydenhuollon tietuetta vaarantui päivittäin. (Alder, 2024)

Kuva 1. Yli 500 tietueen terveydenhuollon tietomurrot (2009–2004)



Tietomurtojen yleisin syy viimeisen vuosikymmenen aikana on ollut hakkerointi. Vaikka hakkerointi ei ollut yhtä yleistä tietomurtojen syynä 2010-luvun alussa, siitä on tullut merkittävin uhka. Tämä osittain johtuu siitä, että terveydenhuollon organisaatiot ovat parantaneet kykyään tunnistaa hakkerointiin liittyvät tietomurrot ja tietoturva-aukot. Esimerkiksi vuonna 2023 hakkerointi muodosti 79,7 % kaikista raportoiduista tietomurroista,

kun taas vuonna 2019 vastaava osuus oli 49 %. Hakkerointiin liittyvien tietomurtojen kasvu on ollut valtavaa, sillä vuosina 2018–2023 ne lisääntyivät peräti 239 %. Lisäksi kiristyshaittaohjelmahyökkäykset ovat olleet merkittävässä roolissa, ja niiden osuus on kasvanut 278 % samana ajanjaksona. (Alder, 2024)

Suomessa on tapahtunut myös merkittäviä kyberhyökkäyksiä, jotka ovat vaikuttaneet niin julkisiin kuin yksityisiin toimijoihin. Yksi Suomen suurimmista ja vakavimmista tietomurroista oli psykiatriakeskus Vastaamoon kohdistunut hyökkäys vuonna 2020. Hyökkääjät varastivat tuhansien potilaiden arkaluonteiset tiedot ja kiristivät sekä yritystä että potilaita. Potilaille lähetettiin uhkausviestejä, joissa vaadittiin lunnaita, ja monien henkilökohtaiset tiedot vuodettiin verkkoon. Tämä tapaus korosti tietoturvan merkitystä erityisesti terveydenhuollossa ja johti julkiseen keskusteluun potilastietojen suojaamisesta. (Hämäläinen, 2021; Tietosuojakeskus, n.d.)

Hyvinvointialueilla tapahtuu vuosittain tietosuoja- ja tietoturvaloukkauksia. Vuonna 2023 Keski-Uudenmaan hyvinvointialueella raportoitiin HaiPro-järjestelmän kautta yhteensä 342 poikkeamaa, joista 73 ilmoitettiin myös tietosuojavaltuutetulle. Keski-Uudenmaan hyvinvointialueella ilmoitus tietosuojavaltuutetulle tehdään aina, kun henkilötietoja on päätynyt ulkopuolisille tahoille. Monissa tapauksissa kyse on ollut virheellisesti väärälle henkilölle toimitetusta asiakirjasta. Ilmoitus rekisteröidylle, eli henkilölle, jota tietoturvaloukkaus koskee, tehdään aina, kun loukkaus todennäköisesti aiheuttaa merkittävän tai korkean riskin henkilön oikeuksille ja vapauksille. (Keusote, 2024).

Vuonna 2017 laajalle levinnyt WannaCry-kiristyshaittaohjelma vaikutti myös Suomeen, ja se löytyi muun muassa Turun yliopistollisen keskussairaalan (TYKS) tietojärjestelmistä. Haittaohjelma aiheutti merkittäviä häiriöitä ympäri maailman, ja Suomessa se paljasti terveydenhuollon IT-järjestelmien haavoittuvuudet. Onneksi suuremmilta vahingoilta vältyttiin, mutta tapaus toi esiin tarpeen parantaa kyberturvallisuuskäytäntöjä. (Keränen, 2017)

Kesäkuussa 2017 Kelan Kanta-palvelut joutuivat jälleen palvelunestohyökkäysten kohteeksi, mikä aiheutti häiriöitä erityisesti Kanta.fi- ja Omakanta-palvelujen käytössä. Hyökkäys vaikutti myös sähköisten reseptien ja potilastiedon arkiston toimintaan julkisen internet-yhteyden kautta. Vaikka häiriö kosketti joitakin pieniä apteekkeja, Kelan mukaan suurempia vaikutuksia ei ollut, ja tietoturva ei ollut vaarassa. (Rautio, 2017)

Hyvinvointialueet ovat havahtuneet kyberturvallisuuden- ja tietosuojakoulutuksen merkityksestä. Monet hyvinvointialueet tarjoavat henkilöstölleen tietosuoja- ja tietoturvaohjeistuksia ja koulutuksia ehkäisemään tietosuojaloukkauksia ja kyberhyökkäyksiä tulevaisuudessa. Terveydenhuollon henkilöstön kyberturvallisuusosaamista voi kehittää Oppiportin tietoturvakoulutuksilla ja Digi- ja väestöviraston Digiturvallinen elämä -koulutuksilla. Näitä lyhyitä koulutuksia voi hyödyntää esimerkiksi perehdytyksessä, ja ne tarjoavat taitoja toimia turvallisesti digitaalisessa ympäristössä. (Vertainen ym., 2024)

2.2.2 Sairaanhoitajan rooli kyberturvallisuudessa

Hoitohenkilökunnan ensisijaisena vastuuna on potilaiden terveyden ja turvallisuuden varmistaminen, mikä kattaa asianmukaisen hoidon sekä potilastietojen luottamuksellisen ja tarkan käsittelyn. Tämä edellyttää eettisten periaatteiden ja lainsäädännön, kuten tietosuoja-asetusten, noudattamista. Hoitohenkilökunnan tulee tunnistaa ja raportoida mahdolliset poikkeamat ja vaaratilanteet, kuten tietoturvaloukkaukset, sekä osallistua jatkuvaan ammatilliseen kehittymiseen potilasturvallisuuden edistämiseksi. (STM, 2019)

Sairaanhoitajan tehtäviin kuuluu potilaiden kohtaaminen ja kuunteleminen, mutta nykyään myös digitaalisten palveluiden ja teknologian käyttö on keskeistä. Sairaanhoitaja opastaa asiakkaita digitaalisten terveyspalvelujen, kuten esitietokyselyiden ja mittaus- ja oiretietojen tallentamisen, hyödyntämisessä. Hän hallitsee monia tietojärjestelmiä, arvioi terveystiedon laatua ja osallistuu moniammatillisiin tiimeihin palveluiden kehittämisessä. Eettisyys ja turvallisuus ovat avainasemassa, ja sairaanhoitaja varmistaa asiakkaan tietosuojan ja -turvan. Näin ollen hän tukee asiakkaita aktiivisessa omahoidossa ja varmistaa, että digitaaliset palvelut ovat kaikkien saatavilla ja edistävät kansalaisten hyvinvointia. (Sairaanhoitajat, 2021)

Sairaanhoitajan kuin myös jokaisen organisaatiossa työskentelevän työntekijän velvollisuus on tutustua tietoturvaohjeistuksiin ja sisäistää ne. Virheellistä toimintaa ei voida perustella tietomättömyyteen vedoten. Omaa vastuuta ei voi siirtää toiselle työntekijälle tai esihenkilölle. Tietoturvallisuusohjeistuksen laiminlyöminen voi johtaa vakaviin tietoturvahäiriöihin ja asiakasturvallisuuden vaarantumiseen. Tietosuojaloukkaukset voivat johtaa rikosoikeudellisiin seuraamuksiin. (Norja ym., 2024)

Sairaanhoitajan työssä kyberturvallisuusuhat ovat erityisen merkittäviä potilastietojen käsittelyssä ja tietojärjestelmien käytössä. Tietomurrot, joissa potilastietoja vuotaa ulkopuolisille, voivat aiheuttaa vakavia seurauksia potilasturvallisuudelle ja yksityisyydelle.

Esimerkiksi sairaanhoitaja, joka kirjaa tai käsittelee potilastietoja sähköisessä potilastietojärjestelmässä, voi joutua tietovuotojen kohteeksi, jos järjestelmä hakkeroidaan. Kiristyshaittaohjelmat ovat toinen yleinen uhka, joka voi lamauttaa koko sairaalan järjestelmät ja hidastaa kriittisiä hoitotoimenpiteitä. Lääkinnällisten laitteiden, kuten hengityslaitteiden tai leikkausrobotin, kyberhyökkäys voi puolestaan johtaa vakaviin potilasturvallisuusriskeihin, kuten virheelliseen lääkeannosteluun tai hengityslaitteen vikaantumiseen leikkauksen aikana. (Vertainen ym., 2024)

Tehtävät ja työympäristöt, joissa kyberuhat ovat erityisen yleisiä, liittyvät sairaanhoitajan päivittäiseen tietojärjestelmien ja sähköisten laitteiden käyttöön. Etätyö, kuten etävastaanottojen pitäminen, on toinen riski, sillä suojaamattomat verkot ja heikosti suojatut laitteet altistavat sairaanhoitajan ja potilaiden tiedot hakkereille. Sähköpostin käyttöön liittyvät phishing-hyökkäykset ovat myös vakava uhka, jossa huijausviesteillä yritetään kalastella sairaanhoitajan kirjautumistietoja tai muuta arkaluontoista tietoa. Lisäksi monissa sairaalaympäristöissä käytetään IoT-laitteita, kuten lääkintälaitteita ja tietokoneita, jotka voivat olla alttiita hyökkäyksille ja tietomurroille. (Vertainen ym., 2024)

2.3 Kyberhyökkäysmetodeja terveydenhuollossa

2.3.1 Tietojen kalastelu

Tietojen kalastelu eli phishing on huijausmenetelmä, jossa rikolliset yrittävät huijata ihmisiä luovuttamaan arkaluonteisia tietoja, kuten salasanoja tai maksutietoja. Rikolliset esiintyvät usein luotettavana tahona, esimerkiksi pankkina tai tunnettuna verkkopalveluna ja houkuttelevat uhrin klikkaamaan haitallista linkkiä tai täyttämään väärennetyn lomakkeen. (F-Secure, 2024b)

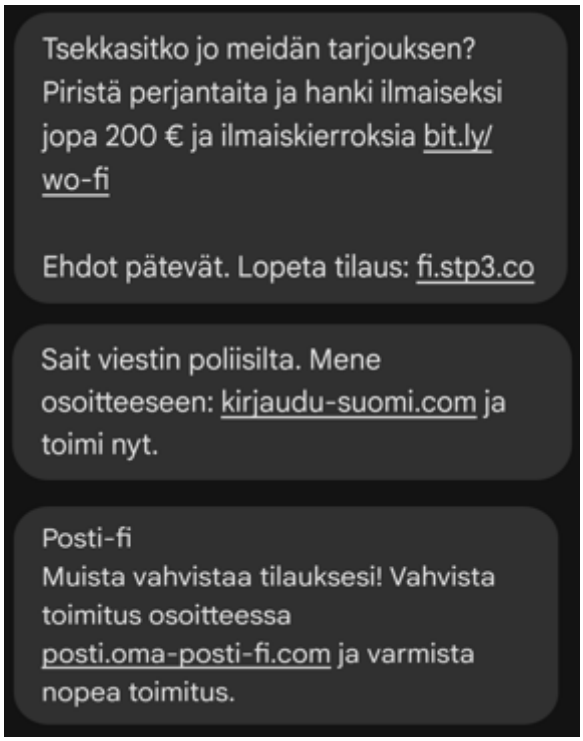
Tietojen kalastelu on yleisin kyberturvallisuusuhka terveydenhuollossa ja yli 90 % kaikista terveydenhuoltoa vastaan kohdistuvista kyberhyökkäyksistä toteutuu tietojenkalasteluhuijausten muodossa (Herjavec Group, n.d.). HIPAA Journalin mukaan 45 % terveydenhuollon kyberturvallisuuden asiantuntijoista on raportoinut, että tietojenkalasteluhyökkäys on ollut heidän organisaationsa pahin tietoturvaloukkaus (HIPAA Journal, n.d.). Sonic Wallin vuoden 2023 kyberuhkaraportissa todettiin, että vuonna 2022 tietojenkalastelu terveydenhuoltoalalla on ollut nousussa. Tietojenkalasteluhyökkäykset keskittyivät kyseisenä vuonna erityisesti talouteen, terveyteen ja kryptovaluuttoihin liittyviin teemoihin. (Sonic Wall, 2023)

Hyökkäykset toteutuvat useilla eri tavoilla: 71 % tapauksista liittyi yleisiin sähköpostihuijauksiin, 67 % kohdennettuihin spear-phishing-hyökkäyksiin, 27 % äänihuijauksiin (vishing), 27 % whaling-hyökkäyksiin, 23 % liiketoimintaan liittyviin sähköpostihuijauksiin, 21 % SMS-huijauksiin, 20 % huijaussivustoihin, 16 % sosiaalisen median huijauksiin, 3 % pharming-hyökkäyksiin ja 2 % syvävääreennyksiin (deepfake). (HIPAA Journal, n.d.)

Tietojen kalastelua voidaan tehdä monin keinoin, kuten sähköpostitse, tekstiviesteillä tai puhelimitse. Esimerkiksi sähköpostilla saat viestin, joka näyttää tulevan pankiltasi ja pyytää sinua päivittämään tilitietosi linkin kautta. Tekstiviestissä voi olla tarjous, joka vaatii klikkaamaan linkkiä osallistumista varten, mutta se ohjaa kalastelusivulle. Puhelimitse tapahtuvassa kalastelussa soittaja voi esiintyä luotettavana tahona, kuten viranomaisena, ja pyytää henkilökohtaisia tietoja. Näiltä hyökkäyksiltä voi suojautua tunnistamalla epäilyttävät viestit ja olemaan jakamatta luottamuksellisia tietoja. (Microsoft, 2024c)

Tietojenkalasteluviestit voi tunnistaa useista varoitusmerkeistä, kuten epäilyttävistä sähköposteista, joissa pyydetään henkilökohtaisia tietoja. Yleensä lähettäjää ei tunneta tai sähköpostiosoite näyttää epäilyttävältä, vaikka viesti näyttäisi tulevan luotettavalta taholta, kuten pankilta. Viesti ei ole henkilökohtainen ja se on usein huonolla suomella kirjoitettu. Sisällössä saatetaan varoittaa kiireellisestä uhasta tai luvata rahallista hyötyä, ja viestissä voi olla linkki, joka vie sivustolle, jossa kysytään luottamuksellisia tietoja. (Kyberturvallisuuskomitea, 2017) Alla olevassa kuvassa 2 on esimerkkejä kalastelutekstiviesteistä.

Kuva 2. Tietojenkalastelu tekstiviestit



Tietojenkalastelun estämisessä on tärkeää noudattaa muutamia keskeisiä käytäntöjä Sähköpostiviestien lähettäjän nimeen ei tule luottaa pelkästään, vaan sähköpostiosoite tulee tarkistaa ennen viestin avaamista, sillä nimi voi olla huijattu. Kirjoitusvirheet on syytä huomioida, koska ne ovat yleisiä kalastelusähköposteissa. Merkittäviä kielioppivirheitä sisältävät viestit tulisi merkitä epäilyttäviksi. Linkin kohdalla on hyvä viedä hiiriosoitin sen päälle ja varmistaa, että osoite näyttää luotettavalta ennen napsauttamista. Jos sähköposti on osoitettu yleisellä nimellä, kuten "Arvokkaalle asiakkaalle", se voi viitata huijaukseen, ja asiaan tulisi suhtautua varovaisesti. Myös sähköpostin alatunnisteen yhteystiedot on tarkistettava, sillä oikeat lähettäjät sisällyttävät ne aina viestiinsä. Pelkoa herättäviin viesteihin, kuten ilmoituksiin tilin sulkemisesta, on syytä suhtautua erityisen tarkkaavaisesti, koska ne ovat tyypillisiä kalasteluhyökkäyksissä. Näitä käytäntöjä noudattamalla voidaan parantaa suojautumista tietojenkalastelulta. (Microsoft, 2024c)

Monivaiheisen tunnistautumisen (MFA) käyttöönotto on yksi tehokkaimmista tavoista suojautua tietojenkalastelua ja tilimurtoja vastaan. MFA avulla pelkkä käyttäjätunnuksen ja salasanan tietäminen ei riitä kirjautumiseen, sillä järjestelmä vaatii lisäksi toisen vahvistustavan, kuten kertakäyttöisen koodin, biometrisen tunnisteen (esim. sormenjälki tai kasvojentunnistus) tai fyysisen todennuslaitteen, kuten USB-avaimen. Tämä lisäsuojaus on erityisen tärkeä palveluissa, joissa käsitellään henkilö- tai maksutietoja, ja se tekee rikollisten

pääsyn tileille huomattavasti vaikeammaksi. Kyberturvallisuuskeskuksen asiantuntijat suosittelevat, että organisaatiot ottavat MFA käyttöön erityisesti ulkoisten yhteyksien kautta käytettävissä palveluissa, kuten pilvipohjaisissa sähköpostipalveluissa, mahdollisimman nopeasti. (Traficom, 2023)

Jos tietojenkalastelun uhriksi joudutaan, on tärkeää toimia nopeasti. Ensin tulee kirjata ylös kaikki hyökkääjälle mahdollisesti jaetut tiedot, kuten käyttäjänimet, salasanat, tilinumerot tai muut henkilökohtaiset tiedot. Tämän jälkeen suositellaan vaarantuneiden tilien salasanojen vaihtamista ja varmistamista, ettei samoja salasanoja käytetä muissa palveluissa. Tietomurrosta on tärkeää ilmoittaa asiaan liittyville tahoille, jotta tarvittavat suojaustoimenpiteet voidaan aloittaa. Mikäli kalastelun seurauksena on menetetty rahaa tai on joutunut identiteettivarkauden uhriksi, poliisille on syytä tehdä välittömästi ilmoitus ja antaa kaikki mahdolliset tiedot tapahtuneesta. Koska tiedot voivat levitä nopeasti rikollisten keskuudessa, on suositeltavaa olla valppaana tulevien tietojenkalasteluviestien varalta. (Microsoft, 2024c)

2.3.2 Kohdistettu tietojen kalastelu

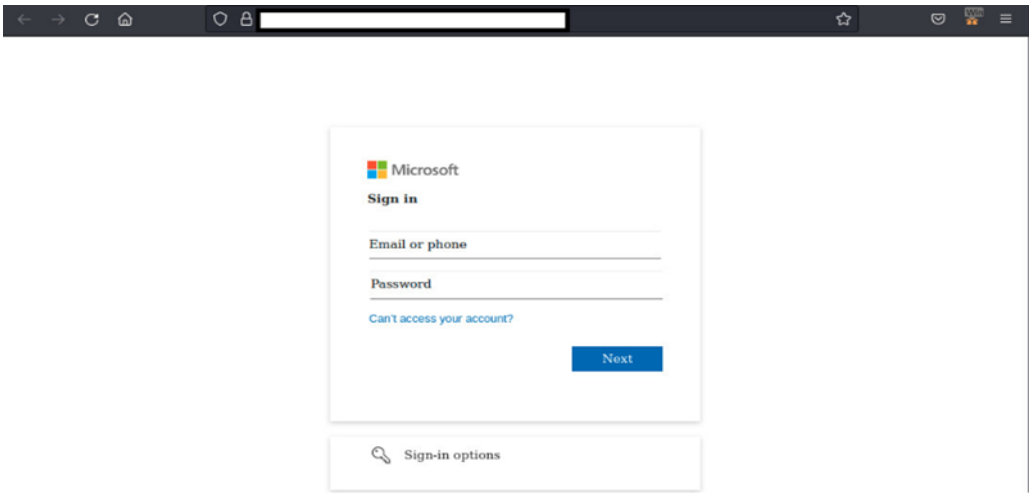
Sosiaali- ja terveydenhuollon organisaatioissa henkilöstö on usein alttiina tietojenkalasteluyrityksille, jotka saapuvat sähköpostin kautta. Esimerkiksi voi tulla viesti, jonka aiheena on "Ladattu asia kirja". Tässä viestissä on linkki, joka näyttää Microsoft SharePointin kirjautumissivulta, mutta todellisuudessa se ohjaa täysin eri osoitteeseen. Kun uhri syöttää käyttäjätunnuksensa ja salasanansa tähän väärentämäänsä kirjautumissivuun, tiedot päätyvät huijarille. Tämä mahdollistaa huijarille organisaation sähköpostitilin haltuunoton. Haltuun otettuja tilejä voidaan käyttää esimerkiksi laskutuspetoksiin, identiteettivarkauksiin tai haitallisen sisällön levittämiseen. Tällaiset hyökkäykset korostavat tarvetta kouluttaa henkilöstöä tunnistamaan epäilyttävät viestit ja suojelemaan omia kirjautumistietojaan. (STM, 2019)

Turvasähköpostihuijaukset ovat edelleen yleisiä ja ne muodostavat merkittäviä riskejä terveydenhuollon organisaatioille. Nämä huijausviestit on suunniteltu näyttämään virallisilta turvapostiviesteiltä, ja ne hyödyntävät usein aitoja logoja ja visuaalisia elementtejä, jotka lisäävät niiden uskottavuutta. Kuvassa 3 on esitetty esimerkki tällaisesta turvapostihuijauksesta. Viestissä saatetaan esimerkiksi väittää, että käyttäjän on pakko vahvistaa tilitietonsa tai päivittää salasanansa ja siihen sisältyy linkki, joka näyttää aidolta kirjautumissivulta, kuten Microsoft 365:ssä. Kuvassa 4 on esimerkki Microsoft-teemaisesta kalastelusivustosta. Kun uhri klikkaa tätä linkkiä ja syöttää sähköpostitunnuksensa sekä

salasanansa, tiedot päätyvät huijarille, joka saa näin käyttöönsä organisaation sähköpostitilin. Tämä voi johtaa laskutuspetoksiin, identiteettivarkauksiin ja uusien kalasteluviestien lähettämiseen muille. Tällaiset hyökkäykset leviävät nopeasti, sillä ne usein tulevat aiemmin murretuilta sähköposteilta, mikä lisää niiden uskottavuutta entisestään. (Traficom, 2023)

Kuva 3. Turvapostikalasteluviesti (Traficom, 2023)

Kuva 4. Microsoft-teemainen kalastelusivusto (Traficom, 2023)



2.3.3 Kiristysohjelma

Kiristyshaittaohjelma on haittaohjelma, joka lukitsee käyttäjän tiedostot tai järjestelmän ja vaatii maksua tiedostojen vapauttamiseksi. Ihmisen ohjaamat kiristyshaittaohjelmat hyödyntävät kohdistettuja hyökkäyksiä, joissa hyökkääjät murtautuvat järjestelmiin, ottavat haltuun kriittisiä resursseja ja leviävät manuaalisesti eri laitteisiin ennen kiristysvaatimusten esittämistä. Tämä lisää uhkan vakavuutta ja vahinkojen laajuutta. (Microsoft, 2024f)

Hyökkääjä vaatii uhrilta rahaa usein virtuaalivaluutassa, lupauksella, että tiedot vapautetaan maksun jälkeen. Haittaohjelmat voivat levitä esimerkiksi huijaussähköpostien kautta tai saastuneiden verkkosivustojen kautta. Organisaatiot, kuten sairaalat ja yritykset, ovat erityisen houkuttelevia kohteita, koska ne eivät voi pysähtyä toiminnassaan ja saattavat siksi maksaa vaaditut lunnaat nopeammin. (Vertainen ym., 2024)

Kiristyshaittaohjelman tunnistaa usein siitä, että käyttäjän tietokone tai tiedostot salataan yhtäkkiä, ja näytölle ilmestyy viesti, jossa vaaditaan lunnaita salauksen purkuavainta vastaan. Usein haittaohjelma leviää sähköpostin liitetiedostoina tai vaarallisina linkkeinä, joita klikkaamalla haittaohjelma aktivoituu. (Vertainen ym., 2024) Erilaisia merkkejä voivat olla myös tietokoneen hidastuminen tai ohjelmistojen virheelliset toiminnat (Healthcare Cybersecurity, 2023). Kiristyshaittaohjelma, kuten WannaCry (kuva 5) toimii tällä tavalla ja pyytää käyttäjää maksamaan lunnaita Bitcoin kryptovaluuttana tiedostojen palauttamista vastaan.

Kuva 5. Kiristyshaittaohjelma WannaCry (BBC, 2017)

Kiristyshaittaohjelmia voidaan estää useilla ennakoivilla keinoilla ja oikeilla toimintatavoilla. Keskeistä on pitää kaikki tietojärjestelmät ja ohjelmistot ajan tasalla, sillä monia hyökkäyksiä hyödynnetään vanhojen haavoittuvuuksien kautta. Lisäksi virustorjuntaohjelmien ja palomuurien käyttö on tärkeää, sillä ne suojaavat järjestelmiä haittaohjelmilta. (Vertainen ym., 2024).

Säännöllinen tietojen varmuuskopiointi on tärkeä toimenpide, joka suojaa tietoja mahdollisilta hyökkäyksiltä. Jos järjestelmä joutuu kyberhyökkäyksen kohteeksi, voit palauttaa tiedot ilman, että sinun tarvitsee maksaa lunnaita. Ennen varmuuskopioinnin aloittamista on kuitenkin tärkeää varmistaa, että valitsemasi verkkopalvelu on hyväksytty IT-osastoltasi. Tämä takaa, että tietosi ovat turvassa ja varmuuskopiointi tapahtuu luotettavassa ympäristössä. (Cybersecurity for the Clinician, 2023)

Organisaatiossa henkilökunnan kouluttaminen tunnistamaan haitalliset sähköpostit, liitteet ja linkit on tärkeä ennaltaehkäisykeino, sillä monet kiristyshaittaohjelmat leviävät sähköpostien kautta (Ontrack, 2022). Koulutus lisää tietoisuutta erilaisista kyberuhista, kuten kiristyshaittaohjelmista, ja niiden toimintatavoista. Kun käyttäjät tunnistavat mahdolliset uhat, he osaavat toimia ennaltaehkäisevästi ja reagoida tehokkaasti poikkeamatilanteissa. Lisäksi koulutus vähentää inhimillisten virheiden mahdollisuutta, kun työntekijät oppivat parhaita käytäntöjä tietojen käsittelyyn liittyen. Koulutuksen myötä syntyy myös vahvempi kyberturvallisuuskulttuuri organisaatiossa, jolloin tietoturva ei ole vain IT-osaston vastuulla, vaan jokaisen työntekijän yhteinen huolenaihe. (Traficom, 2022a)

Käyttäjäoikeuksien rajoittaminen on tärkeä osa tietoturvaa, koska se vähentää merkittävästi riskiä, että haittaohjelma tai muu uhka voi levitä järjestelmään. Kun käyttäjillä on vain peruskäyttöön tarvittavat oikeudet, haittaohjelmat eivät pysty tekemään järjestelmätason muutoksia tai laajasti leviämään verkossa. Tämä rajoittaa myös tahattomien virheiden mahdollisuutta, kuten tärkeiden tiedostojen poistamista tai järjestelmäasetusten muuttamista. Lisäksi, kun käyttäjällä ei ole pääkäyttäjäoikeuksia, haittaohjelmat eivät pysty hyödyntämään näitä oikeuksia päästäkseen syvemmälle järjestelmään. Noudattamalla vähimmän oikeuden periaatetta varmistetaan, että käyttäjillä on vain ne oikeudet, joita he tarvitsevat työnsä suorittamiseen, mikä suojaa tehokkaasti laajempaa verkkoa ja sen kriittisiä tietoja. (Traficom, 2022a)

Vaikka kiristyshaittaohjelma vaatisi lunnaita, niiden maksamista ei suositella, koska tiedostojen palautumisesta tai ongelman ratkeamisesta ei ole mitään varmuutta. Maksaminen voi rohkaista rikollisia pyytämään lisää rahaa tai toistamaan hyökkäyksen.

Lisäksi lunnaiden maksaminen tukee rikollista toimintaa ja edistää kiristyshaittaohjelmien leviämistä. (Traficom, 2022a)

2.3.4 Kyberuhat tulevaisuudessa

Traficomin kuukausittaisessa kybersääjulkaisussa nostetaan esille viisi merkittävintä pitkän aikavälin kyberturvallisuusuhkaa, jotka voivat vaikuttaa yhteiskunnan kyberturvallisuuteen tulevaisuudessa. Näitä uhkia ovat kiristyshaittaohjelmat, tietojen kalastelu, tietomurrot, IoT-laitteiden haavoittuvuudet sekä pilvipalveluihin kohdistuvat hyökkäykset, joissa hyökkääjät hyödyntävät pilviympäristöjen konfigurointivirheitä pääsytietoihin. (Traficom, 2024b)

Tulevaisuudessa myös sosiaali- ja terveydenhuollossa kyberuhat kehittyvät entistä monimuotoisemmiksi ja vaarallisemmiksi. Kiristyshaittaohjelmat säilyvät merkittävänä uhkana, sillä ne voivat estää pääsyn potilastietoihin ja vaarantaa hoidon jatkuvuuden. Tietojenkalasteluyritykset, joissa rikolliset huijaavat henkilöstöä antamaan käyttäjätunnuksia ja salasanoja, lisäävät riskiä vakaviin tietoturvaloukkauksiin. Lääkintälaitteiden etäyhteydet parantavat hallintaa ja korjausmahdollisuuksia, mutta samalla altistavat laitteet hyökkäyksille, mikä korostaa tiukkojen tietoturvatoimien tarvetta. IoT-laitteet, joita käytetään yhä enemmän kotihoidossa, voivat olla haavoittuvia hyökkäyksille, erityisesti kun ne kytkeytyvät internetiin vaihtelevissa ympäristöissä. Palvelunestohyökkäykset pilvipohjaisiin järjestelmiin, kuten potilas- ja asiakastietojärjestelmiin, sekä ihmisten tekemät virheet järjestelmien käytössä lisäävät entisestään riskejä sosiaali- ja terveydenhuollon kentällä. Koulutuksen ja tietoisuuden lisääminen kyberuhista tulee olemaan ratkaisevana haasteiden hallitsemiseksi tulevaisuudessa. (STM, 2019)

Tekoäly tulee muuttamaan merkittävästi myös kyberrikollisuuden kenttää. Rikollisessa toiminnassa hakkerit hyödyntävät tekoäly teknologiaa monin tavoin parantaakseen hyökkäysten tehokkuutta ja monimutkaisuutta. Yksi keskeisistä alueista, jossa tekoälyä hyödynnetään, on tietojenkalastelu, jossa tekoäly voi analysoida uhrin henkilökohtaisia tietoja ja räätälöidä viestit entistä vakuuttavammiksi, mikä parantaa mahdollisuuksia saada arkaluontoisia tietoja, kuten kirjautumistietoja tai pankkitietoja. Toinen merkittävä sovellus on automaattinen haavoittuvuusskannaus, jossa tekoälyä käytetään verkkosivustojen ja sovellusten heikkojen kohtien löytämiseen nopeasti ja tehokkaasti, mikä mahdollistaa näiden heikkouksien hyödyntämisen hyökkäyksissä. (Simplilearn, 2024)

Tekoälyn avulla kehitetään myös älykkäämpiä haittaohjelmia, jotka voivat mukautua ja reagoida ympäristöönsä. Tämä tarkoittaa, että AI-pohjaiset haittaohjelmat voivat muuttaa

koodiaan estääkseen havaintojen ja torjuntatoimien onnistumisen sekä oppia sopeutumaan erilaisten suojausmenetelmien ohittamiseen. Lisäksi tekoäly mahdollistaa deepfake-teknologian käytön, jolla voidaan luoda uskottavia valevideoita ja -äänitteitä. Näiden avulla rikolliset voivat huijata ihmisiä uskomaan väärään tietoon tai tunnistamaan henkilöitä väärin, mikä voi johtaa identiteettivarkauksiin tai huijausyrityksiin. (Traficom, 2024a, 2024d)

Automatisoidut kyberhyökkäykset ovat toinen tekoälyn tuoma kehitys, jossa AI-pohjaiset työkalut voivat suorittaa jatkuvia ja monimutkaisempia hyökkäyksiä ilman jatkuvaa ihmiskäsittelyä, parantaen hyökkäysten tehokkuutta ja nopeutta. Lisäksi tekoäly voi analysoida sosiaalisen median ja muiden verkkosivustojen sisältöä luodakseen tarkkoja profiileja uhreista. Näiden tietojen avulla rikolliset voivat suunnitella entistä tarkemmin kohdennettuja sosiaalisen manipuloinnin hyökkäyksiä, jotka ovat vaikeampia havaita ja torjua. Yhdessä nämä tekoälyn sovellukset tekevät kyberrikollisuudesta monimutkaisempaa ja haastavampaa torjua, korostaen tarvetta kehittää jatkuvasti tehokkaita kyberturvallisuustoimenpiteitä. (Simplilearn, 2024)

2.4 Käytännön keinot suojautua hoitotyössä

2.4.1 Salasanat

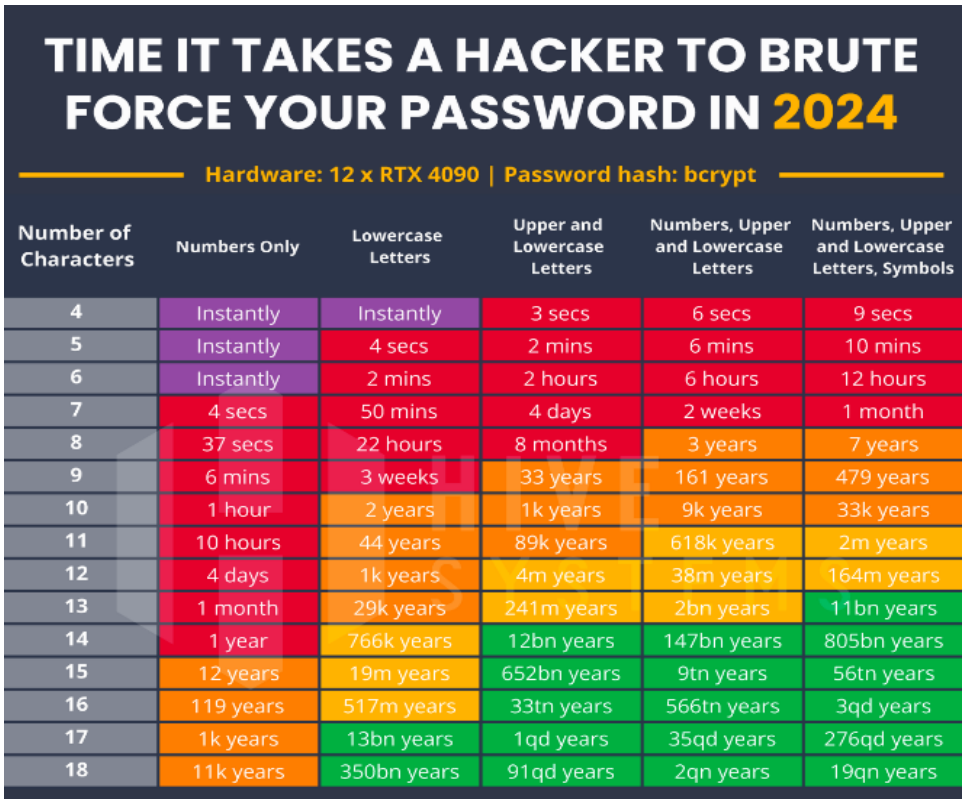
Verkkotilien suojaaminen alkaa vahvojen salasanojen luomisesta. Vahva salasana on vähintään 12 merkkiä pitkä ja sisältää isoja ja pieniä kirjaimia, numeroita sekä symboleja. Sen tulisi olla vaikeasti arvattava, eikä sen tulisi liittyä henkilöihin tai tunnettuihin sanoihin. Tällainen Helppo muistettava salasana voisi olla esimerkiksi 5BlueGiraffes@Jump!. (F-Secure, 2024d)

Tärkeitä käytäntöjä ovat salasanojen jakamisen välttäminen, luotettavien viestintäkanavien käyttö sekä ainutlaatuisten salasanojen käyttäminen eri verkkosivustoilla. Salasanojen hallintatyökalut voivat auttaa tallentamaan ja suojaamaan salasanoja ja kirjallisina muistiinpanoina niitä voi pitää vain turvallisessa paikassa. Salasanojen sijasta voi myös käyttää vihjeitä, jotka auttavat muistamaan salasanan. (Microsoft, 2024b)

Hive Systems -taulukossa (kuva 6) esitetään testituloksia eri laitteistoilla ja hajautusmenetelmillä, mikä auttaa arvioimaan, kuinka tehokkaasti laitteisto, kuten RTX 4090 -grafiikkakortti, pystyy suorittamaan erilaisia hash-funktioita. Hash-funktio on algoritmi, joka muuttaa syötetyn tiedon, kuten salasanan, kiinteän pituiseksi, "scrambled" arvoksi, jota

kutsutaan hashiksi. Esimerkiksi bcrypt on erityisesti salasanojen suojaamiseen kehitetty hajautusalgoritmi, joka käyttää monimutkaisempaa laskentaa, mikä tekee sen murtamisesta vaikeampaa. (Hive systems, 2024)

Kuva 6. Järjestelmien salasanataulukko (Hive systems, 2024)



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

Hardware: 12 x RTX 4090 | Password hash: bcrypt

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

2.4.2 Sähköpostin turvallinen käyttäminen

Sähköpostin turvallinen käyttö on keskeinen osa henkilökohtaisten tietojen suojaamista. Ensimmäinen askel kohti turvallista sähköpostin käyttöä on vahvan ja uniikin salasanan luominen. Salasanan tulisi sisältää pieniä ja isoja kirjaimia, numeroita sekä erikoismerkkejä, jotta se olisi mahdollisimman vaikea murtaa. (Kyberturvallisuuskomitea, 2017)

Lisäksi kaksivaiheinen tunnistautuminen lisää merkittävästi tilin suojausta. Kaksivaiheinen tunnistautuminen vaatii salasanan lisäksi toisen tunnistautumistavan, kuten puhelimeen lähetettävän kertakäyttöisen koodin, mikä estää hakkerien pääsyn tilille, vaikka he saisivat salasanan haltuunsa. (Traficom, 2024c)

Toinen tärkeä keino välttää tietojenkalastelua on tarkistaa aina sähköpostin lähettäjän osoite ennen viestin avaamista. Vaikka viestin lähettäjän nimi vaikuttaisi tutulta, sähköpostiosoite

saattaa paljastaa viestin todellisen lähteen. Epäilyttäviltä vaikuttavat viestit, jotka sisältävät tuntemattomia linkkejä tai liitteitä, tulisi jättää avaamatta. Myös liitteiden lataaminen tuntemattomilta lähettäjiltä voi sisältää riskejä, ja viestin tietoturvapalkit (keltaiset tai punaiset) voivat antaa vihjeitä viestin turvallisuudesta. (Microsoft, 2024a)

2.4.3 Työaseman käyttäminen

Työaseman turvallinen käyttö on tärkeä osa tietoturvaa erityisesti hoitotyössä, jossa käsitellään arkaluonteisia henkilötietoja ja potilastietoja. Työaseman turvalliseen käyttöön kuuluu huolellinen kirjautuminen sisään ja ulos potilastietojärjestelmistä. Kun työskentely päättyy, työntekijän on varmistettava, ettei potilastietoja jää näkyville työasemalle, jolloin ne voisivat päätyä sivullisten nähtäväksi. Tämä auttaa suojaamaan sekä potilaiden yksityisyyttä että työnantajan tietoja, mikä on keskeistä tietoturvan ylläpitämisessä hoitotyössä. (Siun SOTE, 2024)

Työaseman lukitseminen on yksinkertainen mutta tehokas tapa estää luvaton pääsy tietoihin, esimerkiksi silloin, kun työntekijä poistuu työpisteeltään hetkeksi. Lukitsemiskomento, kuten Windows-näppäin ja L-kirjain, varmistaa, että vain luvalliset henkilöt pääsevät käsiksi tietoihin. Lisäksi vahvat salasanat, joissa yhdistellään kirjaimia, numeroita ja erikoismerkkejä, ovat keskeinen osa työaseman suojautumista. (Siun SOTE, 2024)

Työaseman käyttäminen henkilökohtaisiin tarkoituksiin, kuten yksityisen sähköpostin tarkistamiseen tai sosiaalisen median selaamiseen, voi lisätä merkittävästi tietoturvariskejä. Työasemat ovat yleensä liitettynä organisaation verkkoon ja sisältävät arkaluonteisia tietoja, kuten potilastietoja tai työnantajan luottamuksellisia tietoja. Henkilökohtaisten palveluiden käyttö voi altistaa työaseman haittaohjelmille tai tietomurroille, sillä yksityiset sähköpostit ja sosiaalisen median alustat voivat olla alttiimpia tietojenkalastelulle ja muille kyberuhkille. Jos työasemalle pääsee esimerkiksi haittaohjelma henkilökohtaisen toiminnan kautta, se voi levitä koko järjestelmään ja vaarantaa potilastietojen ja muiden arkaluonteisten tietojen turvallisuuden. (Siun SOTE, 2024)

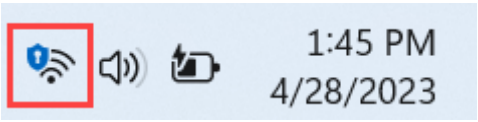
Tietoturvaohjelmistojen käyttö ja säännölliset päivitykset auttavat varmistamaan, että työasema on suojattu mahdollisilta uhkilta, kuten haittaohjelmilta ja tietomurroilta. Erityisen tärkeää on, että työasemat ja niillä käytettävät ohjelmistot ovat aina ajan tasalla, jotta tietoturva pysyy korkealla tasolla. Monilla ohjelmilla on mahdollisuus automaattisiin päivityksiin, jolloin käyttäjän ei tarvitse huolehtia uusimpien versioiden hakemisesta itse (Traficom, 2020a)

VPN-yhteys on tärkeä työkalu sosiaali- ja terveydenhuollon tietoturvan parantamisessa, erityisesti tilanteissa, joissa työntekijät käyttävät julkisia verkkoja tai käsittelevät potilastietoja etänä. VPN salaa tiedonsiirron ja piilottaa käyttäjän IP-osoitteen, jolloin ulkopuoliset eivät pääse käsiksi arkaluonteisiin tietoihin, kuten potilasrekistereihin ja muihin henkilötietoihin. Tämä on erityisen tärkeää, koska sosiaali- ja terveydenhuollon toimijat käsittelevät paljon arkaluonteisia henkilötietoja, joiden suojaaminen on keskeistä paitsi lainsäädännöllisistä syistä, myös organisaatioiden maineen säilyttämiseksi. (STM, 2019)

VPN (Virtual Private Network) on teknologia, joka mahdollistaa internetin käytön turvallisemmin ja yksityisemmin ohjaamalla verkkoyhteytesi VPN-palvelimen kautta. Tämä piilottaa IP-osoitteesi ja todellisen sijaintisi, suojaten yksityisyyttäsi ja estäen ulkopuolisia seuraamasta verkkotoimintaasi, erityisesti julkisissa Wi-Fi-verkoissa. Lisäksi VPN salaa verkkoliikenteesi, mikä tekee siitä näkymättömän hakkereille ja internetpalveluntarjoajille. (F-Secure, 2024a)

VPN-yhteyden muodostaminen onnistuu helposti joko tehtäväpalkista tai Windowsin asetuksista. Voit valita tehtäväpalkista Verkko, Äänenvoimakkuus tai Akku-kuvakkeen, josta pääset VPN-yhteyksien luetteloon. Sieltä valitaan haluttu yhteys ja napsautetaan Yhdistä, minkä jälkeen syötetään tarvittavat kirjautumistiedot. Toinen vaihtoehto on mennä Asetukset-valikossa kohtaan Verkko & Internet ja valita VPN-yhteys, jonka vieressä painetaan Yhdistä. Onnistuneen yhteyden tunnistaa siitä, että VPN-yhteyden nimi näkyy yhdistettynä asetuksissa, ja tehtäväpalkissa näkyy sininen kilpi (ks. kuva 7). (Microsoft, 2024e).

Kuva 7. Tehtäväpalkin kuvake VPN-yhteydestä



2.4.4 Varmuuskopiointi

Varmuuskopioinnilla tarkoitetaan tärkeiden tiedostojen ja tietojen kopiointia alkuperäisen tallennuspaikan lisäksi yhteen tai useampaan paikkaan. Varmuuskopioiden avulla voit palauttaa tiedostot, jos alkuperäiset tiedot katoavat tai vahingoittuvat. Tämä on tärkeää erityisesti tilanteissa, joissa tallennusväline, kuten tietokoneen kiintolevy tai USB-muisti, tuhoutuu, virus tuhoaa tiedostoja, tiedostoja poistetaan vahingossa, tai tallennusväline katoaa tai varastetaan. Varmuuskopiointi tulisi tehdä säännöllisesti, ja paras käytäntö on

tallentaa kopiot useisiin eri paikkoihin, kuten pilvipalveluihin tai ulkoisille kovalevyille. Usein suositellaan esimerkiksi päivittäistä varmuuskopiointia, jos tiedostoihin tehdään jatkuvia muutoksia. Näin varmistetaan, että tärkeät tiedot ovat aina saatavilla, vaikka jokin odottamaton tapahtuma sattuisi. (Helsingin yliopisto, 2024)

Varmuuskopiointi on kriittinen osa sosiaali- ja terveydenhuollon (SOTE) tietoturvaa, sillä se varmistaa potilas- ja asiakastietojen turvallisuuden sekä toiminnan jatkuvuuden mahdollisissa häiriötilanteissa, kuten tietojärjestelmien vikaantuessa, tietomurtojen tai kiristyshaittaohjelmien kohteeksi jouduttaessa. SOTE-alalla potilastiedot ovat elintärkeitä, ja niiden menetys voi vaarantaa hoidon laadun ja potilasturvallisuuden. Tehokas varmuuskopiointi noudattaa 3–2–1-sääntöä, jossa tiedot varmuuskopioidaan kolmesti. Tässä käytetään kahta eri tallennusvälinettä ja yksi kopio säilytetään erillisessä sijainnissa. Näin voidaan varmistaa tietojen palautettavuus ja häiriöiden minimoiminen vaikutus, mikä on oleellista erityisesti kriittisten terveyspalveluiden ylläpitämiseksi. (Vertainen ym., 2024)

2.4.5 Kaksivaiheinen tunnistautuminen varmennekortilla

Sote-ammattikortti on terveydenhuollon ammattilaisille tarkoitettu sähköinen varmennekortti, jota käytetään henkilöllisyyden varmentamiseen ja sähköisiin allekirjoituksiin terveydenhuollon tietojärjestelmissä. Kortti varmistaa, että vain valtuutetut henkilöt pääsevät käsittelemään potilastietoja ja muita luottamuksellisia tietoja. Sote-ammattikortti on henkilökohtainen, ja sen käytöstä vastaa aina kortinhaltija itse. Tämä tarkoittaa, että kortti tulee pitää huolellisesti tallessa ja tunnusluvut tulee säilyttää erillään kortista tietoturvariskien minimoimiseksi. (Digi- ja väestötietovirasto, 2024)

Jos sote-ammattikortti vahingoittuu, katoaa tai tulee tarpeettomaksi, siitä tulee välittömästi ilmoittaa sulkupalveluun väärinkäytösten estämiseksi. Kortinhaltijan on suositeltavaa tallentaa kortin numero, jotta kortin sulkeminen voidaan tehdä nopeasti ongelmatilanteissa. Kortin turvallinen käsittely ja säilyttäminen ovat olennaisia, jotta kortin väärinkäytön riski pysyy mahdollisimman pienenä ja tietoturva säilyy korkealla tasolla. (Digi- ja väestötietovirasto, 2024)

2.5 Kyberuhkien ilmoittaminen hoitotyössä

Kyberturvallisuushäiriöiden hallinta alkaa poikkeaman havaitsemisesta kybertoimintaympäristössä. Poikkeama voi ilmetä esimerkiksi ICT-palveluiden häiriönä, sähkökatkona, joka uhkaa niiden toimivuutta, tai salassa pidettävän tiedon paljastumisena. Poikkeaman ilmetessä ensimmäinen askel on arvioida häiriön tyyppi ja mahdollinen vaikutus organisaation toimintaan, tietosuojaan, potilas- tai asiakasturvallisuuteen. Tilanne voi liittyä esimerkiksi potilastietojärjestelmän, lääkintälaitteiden tai tietojen siirron häiriöihin. Tämän arvion perusteella päätetään, onko tarpeen ryhtyä välittömiin toimenpiteisiin. Ilmoitus häiriöstä tehdään organisaation vastuuhenkilöille tai ICT-palveluntarjoajan käyttötukeen. Ensivaiheessa kerättyjen tietojen pohjalta arvioidaan, onko kyse kyberhäiriöstä vai esimerkiksi normaalista tukipyynnöstä. Jos häiriö todetaan kyberhyökkäykseksi, on käynnistettävä vahinkojen rajoittaminen ja varajärjestelmien käyttö harkitaan tilanteen edetessä. (STM, 2019)

Jokaisen työntekijän on velvollisuus ilmoittaa havaitsemastaan tietosuojapoikkeamasta tai sen epäilystä esihenkilölleen tai organisaation turvallisuuspäällikölle. Arvioinnissa on huomioitava poikkeaman mahdolliset vaikutukset henkilötietoihin ja kohteena oleviin henkilöihin. Jos tilanne vaatii, se on käsiteltävä henkilötietojen tietoturvaloukkauksena, ja kaikki tapahtumat on dokumentoitava ja riskiarvioitava. (Siun SOTE, 2024).

Tietosuojapoikkeamasta voidaan tehdä HaiPro-ilmoitus, jos organisaatiolla on tämä järjestelmä käytössään. HaiPro on raportointijärjestelmä, jolla ilmoitetaan potilasturvallisuutta vaarantavista tilanteista, kuten haitta- ja läheltä piti -tilanteista. Sen avulla työntekijät voivat raportoida tapahtumista, jotka ovat aiheuttaneet tai olisivat voineet aiheuttaa haittaa potilaalle, tavoitteena parantaa turvallisuutta ja kehittää toimintaa. Organisaatiosta riippuen HaiPro-järjestelmällä voidaan raportoida myös muita turvallisuusriskejä, kuten tietoturvapoikkeamia. Esimerkiksi potilastietojen luvaton käsittely tulee ilmoittaa viipymättä, jotta toimenpiteisiin voidaan ryhtyä potilasturvallisuuden varmistamiseksi. (HaiPro, 2019)

Tietosuojapoikkeamat ovat tapahtumia, jotka uhkaavat henkilötietojen turvallisuutta ja voivat johtaa niiden tuhoutumiseen, häviämiseen, luvattomaan luovutukseen tai muuhun käsittelyyn ilman asianmukaista oikeutta. Esimerkkejä tietosuojapoikkeamista ovat salassa pidettävien tietojen lähettäminen suojaamattomassa sähköpostissa, asiakas- tai potilastietojen postitus väärälle henkilölle sekä hävinneet tai varastetut tietokoneet tai tiedonsiirtovälineet. Henkilötietojen tietoturvaloukkauksia voivat olla myös hävinneet tiedonsiirtovälineet, kuten USB-tikut, varastetut tietokoneet, hakkerointi, haittaohjelmatartunnat, kyberhyökkäykset,

tulipalot datakeskuksissa sekä tiliotteen postitus väärälle henkilölle. Kaikki tietosuojapoikkeamat, kuten tietojen kalastelu, tietomurrot tai haittaohjelmahyökkäykset, on otettava vakavasti, sillä ne voivat heikentää tietojen eheyttä, luottamuksellisuutta ja saavutettavuutta. (Tietosuojavaltuutetun toimisto, 2024; Pirha, 2024)

2.6 Potilastietojen käsittely ja suojaaminen

Potilastietojen käsittelyllä tarkoitetaan kaikkia toimenpiteitä, joita tehdään potilaan terveydentilaa koskeville tiedoille, kuten tietojen keräämistä, tallentamista, käyttöä, siirtämistä ja poistamista. Potilastietojen käsittely on tarkasti säädeltyä, ja tietoja voidaan käsitellä vain tiettyä käyttötarkoitusta varten, kuten hoidon järjestämiseksi tai lakisääteisten velvoitteiden täyttämiseksi. Erityisesti terveyttä koskevat tiedot kuuluvat erityisiin henkilötietoryhmiin, joiden käsittely on lähtökohtaisesti kielletty, ellei siihen ole suostumusta tai muuta laillista perustetta, kuten terveydenhuollon järjestämiseen liittyvät tehtävät. Potilastietojen käsittelyssä on noudatettava tietosuoja-asetusta ja kansallista lainsäädäntöä, jotka määrittävät tarkat säännöt tietojen käsittelylle, säilyttämiselle ja luovuttamiselle. (THL, 2024a)

Potilastietojen käsittelystä säädetään laissa sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023). Laki yhdenmukaistaa potilas- ja asiakastietojen käsittelyn terveydenhuollossa sekä asettaa tiukat salassapitovelvollisuudet. Potilastiedot ovat pysyvästi salassa pidettäviä, eikä niitä saa näyttää sivullisille ilman laillista perustetta. Terveydenhuollon yksiköissä potilaan hoidon kannalta välttämättömiä tietoja saa käsitellä, mutta tietojen luovuttaminen vaatii potilaan suostumuksen tai laissa määritellyt poikkeustilanteet. (Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 703/2023)

2.6.1 Potilastietojen luovuttaminen

Potilastietojen luovuttaminen on erittäin herkkä ja säädelty prosessi, joka perustuu potilaan oikeuksiin ja yksityisyyden suojaan. Potilastietoja saa luovuttaa ainoastaan potilaan suostumuksella tai lainmukaisista syistä. Tämä tarkoittaa, että ennen potilastietojen jakamista on aina varmistettava, että potilas on antanut siihen suostumuksensa. Poikkeuksena ovat tilanteet, joissa tietojen luovuttaminen on lain mukaan sallittua ilman suostumusta, kuten hätätilanteissa, joissa potilaan hyvinvointi on uhattuna, tai kun lainkäyttöön liittyvät asiat vaativat tietojen antamista. (THL, 2024b) Jos potilas ei kykene antamaan lupaa esimerkiksi muistisairauden, mielenterveyden häiriön tai tajuttomuuden

takia, tietoja voidaan luovuttaa välttämättömien terveyspalvelujen toteuttamiseksi ilman lupaa. (Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 703/2023)

Luovuttaja on vastuussa potilastietojen lainmukaisesta luovuttamisesta. Tämä tarkoittaa, että ennen tietojen luovuttamista, luovuttajan on varmistettava, että kaikki lain vaatimukset täyttyvät. Luovuttaja voi myös pyytää tietojen pyytäjältä lisätietoja, kuten tarkkaa tarkoitusta, johon tietoja aiotaan käyttää, sekä lain perusteita, jotka oikeuttavat tietojen saamiseen. Tämä lisäinformaatio auttaa luovuttajaa arvioimaan, onko tietojen luovuttaminen oikeutettua ja tarpeellista. (THL, 2024)

Potilas voi tarkastella Kanta-palveluun tallennettuja tietojaan OmaKannasta. OmaKanta on potilaalle suunnattu sähköinen palvelu, joka mahdollistaa hänen omien potilastietojensa, kuten lääkityksen ja hoitohistorian, tarkastelun. Tämä ominaisuus vähentää erillisten tietopyyntöjen tarvetta, sillä potilas voi itse päästä käsiksi tarvitsemiinsa tietoihin nopeasti ja helposti. Tällöin potilas voi myös aktiivisesti seurata omaa hoitoaan ja osallistua hoitoprosessiinsa, mikä parantaa hoidon laatua ja potilastyytyväisyyttä. OmaKanta kannustaa potilaita olemaan tietoisia omasta terveydentilastaan ja hoitosuunnitelmistaan. (Siun SOTE, 2024)

2.6.2 Potilastietojen kirjaaminen

Potilastietojen kirjaaminen on olennainen osa terveydenhuollon palvelua ja hoitoa. Potilastietojen tulee olla selkeitä, ymmärrettäviä ja tarpeellisia potilaan hoidon suunnittelun, toteutuksen ja seurannan kannalta. Kirjausten on perustuttava terveydenhuollon ammattihenkilön omiin havaintoihin, ja muiden lähteiden osalta tulee aina mainita tiedon alkuperä. Potilastiedot, kuten käyntikirjaukset ja lähetteet, tulee kirjata viiveettä, viimeistään viiden päivän sisällä potilaan palvelutapahtuman päättymisestä. (Siun SOTE, 2024)

Jokaisessa hoitoprosessin vaiheessa terveydenhuollon ammattihenkilöllä on velvollisuus kirjata potilaan hoitoon liittyvät tarpeelliset tiedot potilasasiakirjoihin. Potilasasiakirjoihin sisältyvät potilaskertomus ja siihen liittyvät tiedot, lääketieteellisiin kuolemansyihin liittyvät asiakirjat sekä muut potilaan hoidon aikana syntyneet tai saapuneet asiakirjat. Potilaskertomuksen merkintöjä jäsennetään asiakokonaisuuksittain eri näkymille, esimerkiksi lääketieteen erikoisalan tai palveluiden mukaan. (THL, 2024a)

Potilaan hoitoon osallistuvat ammattihenkilöt ja opiskelijat voivat tehdä kirjauksia, mutta opiskelijoiden kirjaukset tulee hyväksyä heidän ohjaajansa tai esihenkilön toimesta.

Tietosuojan näkökulmasta potilaalla on oikeus nähdä ja korjata omia tietojaan. Lisäksi, mikäli potilaan itsemääräämisoikeutta rajoitetaan, tulee siitä tehdä merkintä potilastietoihin. Myös puhelinneuvottelut ja konsultaatioiden tulokset on kirjattava, jos ne ovat hoidon kannalta merkittäviä. (Siun SOTE, 2024)

Potilastiedot tallennetaan valtakunnallisiin tietojärjestelmäpalveluihin, kuten Potilastietovarantoon ja Kuva-aineistojen tietovarantoon. Tietojen kirjaaminen tapahtuu rakenteisesti, mikä tarkoittaa, että tiedot tallennetaan yhtenäisellä ja määrämuotoisella tavalla, hyödyntäen koodistoja, luokituksia ja termistöjä. Tämä yhtenäinen kirjaamistapa parantaa tiedon laatua ja kattavuutta, jolloin tietoja voidaan hyödyntää paremmin esimerkiksi uusien asiakirjojen laatimisessa tai yhteenvetojen, lausuntojen ja todistusten pohjana. (THL, 2024a)

3 Opinnäytetyön toteutusmenetelmä

Opinnäytetyö ja tutkimus pohjautui teoreettiseen viitekehykseen, jonka perusteella laadittiin opetusmateriaali sairaanhoitajaopiskelijoille. Tämä materiaali esitettiin opiskelijoille luennon muodossa, minkä jälkeen kerättiin palautetta sen sisällöstä ja luennon onnistumisesta. Palautteen analysoinnin avulla vastattiin tutkimuskysymyksiin: kuinka hyvin sairaanhoitajaopiskelijat ymmärtävät kyberturvallisuuden periaatteet ja niiden soveltamisen hoitotyössä koulutuksen jälkeen? Miten tehokasta opetusmateriaali on opiskelijoiden kyberturvallisuusosaamisen arvioinnissa?

Opinnäytetyö aloitettiin etsimällä vastauksia tutkimuskysymyksiin: Miten hyvin hoitohenkilökunta tuntee tietosuojaan ja kyberturvallisuuteen liittyvät periaatteet? Millaisia kyberuhkia hoitohenkilökunta kohtaa päivittäisessä työssään? Tutkimusmenetelmä perustui kirjallisuuskatsaukseen, jossa kerättiin tietoa hoitohenkilökunnan tietosuoja- ja kyberturvallisuustietoisuudesta sekä heidän kohtaamistaan kyberuhista. Kerätystä tiedosta koottiin teoreettinen viitekehys.

3.1.1 Teoreettisen viitekehyksen aineiston kerääminen ja rajaus

Teoreettisen viitekehyksen lähdeaineisto kerättiin vuosien 2017–2024 väliltä, sillä terveydenhuollon kyberturvallisuuteen liittyvä ajankohtainen tieto on rajallista ennen vuotta 2017. Tällä aikarajauksella pyrittiin varmistamaan, että tutkimus ja opetusmateriaali perustui mahdollisimman tuoreisiin ja relevantteihin tietoihin. Lähdeaineisto käsitteli kyberturvallisuutta hoitotyössä ja terveydenhuollossa koostuen useista eri lähteistä, kuten tutkimusartikkeleista, tieteellisistä julkaisuista, lakiteksteistä, standardeista, raporteista ja tilastoista sekä oppaista.

Lähteiden valintaprosessissa käytettiin sekä suomen- että englanninkielisiä hakusanoja, kuten "kiristyshaittaohjelma", "kyberturvallisuus hoitotyössä", "kyberturvallisuus terveydenhuollossa", "kyberturvallisuus tilasto", "Potilas- ja asiakastietojen ja henkilötietojen käsittely", "tietojen kalastelu", "tietoturva", "cyber security in nursing", "cyber security statistics", "cybersecurity in healthcare", "Information security", "patient and document processing", "Phishing", "ransomware". Aineistoa etsittiin monipuolisesti eri tietokannoista ja hakukoneista, kuten Google ja Google Scholar. Tämä mahdollisti kattavan ja ajankohtaisen aineiston kokoamisen opetusmateriaalin pohjaksi.

3.1.2 Opetusmateriaalin kehittäminen

Teoreettisen viitekehyksen pohjalta laadittiin opetusmateriaali (liite 1), joka suunniteltiin sairaanhoitajaopiskelijoille tarkoitettua luentoa varten. Opetusmateriaalin kehittämisessä käytettiin teoreettisen viitekehyksen kaikkia lähteitä. Materiaali sisältää perusperiaatteita kyberturvallisuudesta hoitotyössä ja käytännön esimerkkejä, jotka liittyvät tietoturvauhkien tunnistamiseen ja ennaltaehkäisyyn sekä kyberuhkien ilmoittamiseen. Tämän lisäksi materiaali sisälsi konkreettisia esimerkkejä, jotka havainnollistivat, miten kyberuhat voivat vaikuttaa terveydenhuollon toimintaan. Materiaalin suunnittelussa huomioitiin kyberturvallisuuden ajankohtaiset kyberturvallisuus haasteet terveydenhuollossa ja kyberuhkien tulevaisuuden näkymät.

3.1.3 Opetusmateriaalin testaaminen ja palaute

Opetusmateriaalia testattiin marraskuussa pidettävällä luennolla, jonka jälkeen opiskelijoilta kerättiin anonyymiä palautetta Webropol-kyselylomakkeen avulla. Kyselyaineisto (liite 2) kerättiin anonyymisti ja tallennettiin Microsoft OneDrive -pilvipalveluun, joka on suojattu Hämeen ammattikorkeakoulun tietoturvapolitiikan mukaisesti. Aineistoa käsittelevät ainoastaan opinnäytetyön tekijä ja ohjaaja. Koska aineisto ei sisällä henkilötietoja, erityisiä tietosuojatoimenpiteitä ei tarvittu.

3.1.4 Opetusmateriaalin ulkoasu

Opetusmateriaalin kuvien luomiseen hyödynnettiin Leonardo AI-kuvageneraattoria, mikä toi visuaalista mielenkiintoa dioihin. AI-kuvageneraattorin käyttö auttoi esityksen visuaalisessa suunnittelussa, korostaen oppimateriaalin tärkeimpiä aiheita ja parantaen opiskelijoiden kokemusta. Kuvageneraattori mahdollisti nopeasti luotujen ja teemaan sopivien kuvien lisäämisen materiaaleihin, mikä teki opetuksesta visuaalisesti selkeämpää ja havainnollisempaa. Seuraavassa käydään läpi kuvien prompteja.

Dioissa 1 - 6 & 23 – 27 käytetty Kuva 9 luotiin seuraavalla promptilla: “Make a picture about modern hospital building. put red hospital logo on the building (Red cross). Write "Hospital" next to logo. Do not show any human”.

Kuva 8. Tekoälyllä generoitu kuva sairaalasta

Dioissa 7 & 9 käytetty Kuva 10 luotiin seuraavalla promptilla: “Make picture about cybersecurity in nursing. don’t make humans in picture. make just a view of something related to cybersecurity”.

Kuva 9. Tekoälyllä generoitu kuva hoitajista

Dia 8 käytetty Kuva 11 luotiin seuraavalla promptilla: “Make a picture about modern hospital building. do not show any human”.

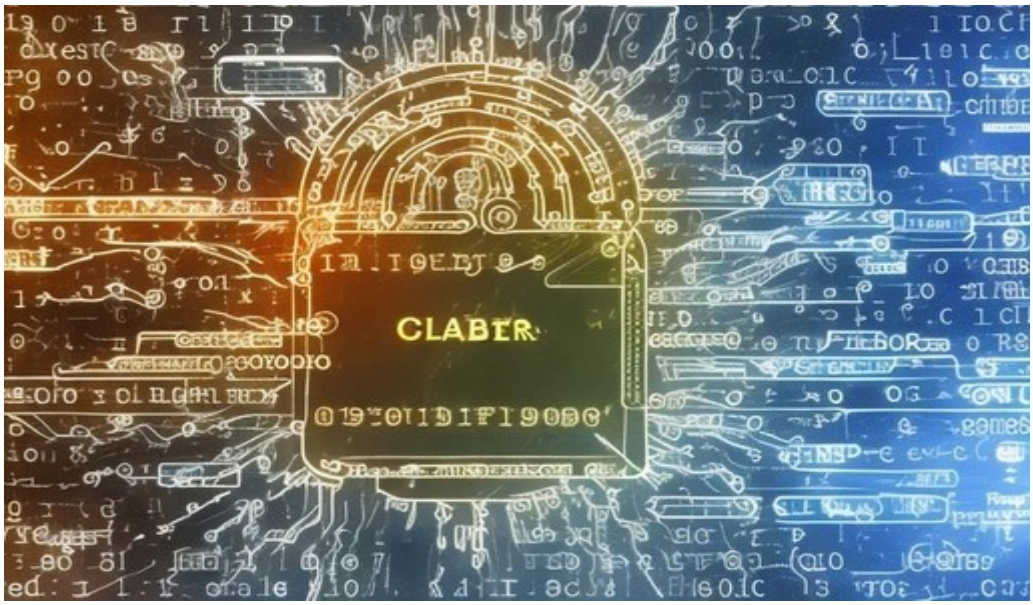
Kuva 10. Tekoälyllä generoitu kuva sairaalan sisätiloista

Dioissa 11-13 käytetty Kuva 12 luotiin seuraavalla promptilla: "Nurse pushing forward bed in hospital hallway. High quality"

Kuva 11. Tekoälyllä generoitu kuva hoitajasta työntämässä sänkyä

Dioissa 14 - 17 käytetty Kuva 13 luotiin seuraavalla promptilla " one nurse moving bed forward in hospital hallway. high quality”.

Kuva 12. Tekoälyllä generoitu kuva lukosta kyberturvallisuudessa



Dioissa 18 - 19 käytetty Kuva 14 luotiin seuraavalla promptilla: "Draw a hospital with a car next to it. Background blue”.

Kuva 13. Tekoälyn generoima kuva sairaalasta

Dioissa 20 - 22 käytetty Kuva 15 luotiin seuraavalla promptilla: " Make a picture of a work desk. Add sunglasses, a card, papers, and a smartphone”.

Kuva 14. Tekoälyllä generoitu kuva työpöydästä

Diassa 18 käytetty kuva 16 Sote ammattikortin naisesta luotiin seuraavalla promptilla: ”Make a portrait of a woman who is smiling.”. Ammattikortin tausta kuvattiin aidosta Soteammattikortista ja kortin henkilötiedot muokattiin paint-ohjelmistolla.

Kuva 15. Tekoälyllä generoitu kuva Sote ammattikortista

4 Tulokset

4.1 Palautekyselyn tulokset

Kyberturvallisuusaiheisen luennon palautekyselyn tulokset esitetään tässä kappaleessa. Luento pidettiin monimuotototeutuksen opiskelijoille torstaina 28.11. Luentoon osallistui kuusi sairaanhoitajaopiskelijaa. Palautekyselyyn vastasi viisi henkilöä, mikä vastaa noin 10 % koko monimuotototeutuksen opiskelijamäärästä (n. 50 opiskelijaa).

Palautekyselyn tulokset:

Ymmärrän, että kyselyyn vastaaminen on vapaaehtoista ja haluan osallistua opinnäytetyön tutkimukseen. kyllä: n=5, 100 %. Kaikki vastaajat hyväksyivät kyselyn ja halusivat osallistua tutkimukseen.

1. Opetusmateriaali (PowerPoint esitys)
1.1 Opetusmateriaalin sisältö oli selkeä ja ymmärrettävä.

Samaa mieltä: 80 % (n=4). Jokseenkin samaa mieltä: 20 % (n=1). Opiskelijat pitivät opetusmateriaalia pääsääntöisesti selkeänä ja ymmärrettävänä, vaikka yksi vastaaja koki materiaalin vain osittain selkeäksi.

1.2 Opetusmateriaalissa esitetyt esimerkit olivat hyödyllisiä.

Samaa mieltä: 100 % (n=5). Kaikki vastaajat arvioivat opetusmateriaalin esimerkit hyödyllisiksi. Tämä korostaa käytännönläheisten esimerkkien merkitystä kyberturvallisuuden opetuksessa.

1.3 PowerPoint-esityksen visuaalinen ilme tuki oppimista.

Samaa mieltä: 80 % (n=4). Jokseenkin samaa mieltä: 20 % (n=1). Valtaosa opiskelijoista oli sitä mieltä, että PowerPoint-esityksen visuaalinen ilme tuki oppimista. Yksi vastaaja koki kuitenkin, että visuaalinen ilme voisi olla vielä selkeytetty tai paranneltu.

2. Luento
2.1 Luennolla esitetyt asiat tukivat kyberturvallisuuden ymmärtämistä hoitotyössä.

Samaa mieltä: 100 % (n=5). Kaikki vastaajat olivat yhtä mieltä siitä, että luennon sisältö tuki kyberturvallisuuden ymmärtämistä erityisesti hoitotyön näkökulmasta.

2.2. Luennoitsijan esitystapa oli selkeä ja mukaansatempaava.

Samaa mieltä: 100 % (n=5). Luennoitsijan esitystapaa pidettiin selkeänä ja mukaansatempaavana. Tämä viittaa siihen, että esitystapa vastasi opiskelijoiden odotuksia ja tuki oppimista.

2.3. Luennon aikana esitetyt kysymykset ja keskustelut olivat hyödyllisiä.

Samaa mieltä: 100 % (n=5). Kaikki vastaajat arvioivat luennon aikana esitetyt kysymykset ja käydyt keskustelut hyödyllisiksi, mikä korostaa interaktiivisuuden merkitystä oppimisessa.

3. Osaamisen arviointi ja kehittyminen
3.1 Arvioi omaa kyberturvallisuustietämystäsi ennen luentoa.

Erittäin hyvä: 40 % (n=2). Hyvä: 40 % (n=2). Heikko: 20 % (n=1). Ennen luentoa vastaajien kyberturvallisuustietämys oli vaihtelevaa. Kaksi vastaajaa arvioi tietonsa erittäin hyväksi ja kaksi hyväksi, mutta yksi arvioi tietämyksensä heikoksi. Tämä viittaa siihen, että osallistujilla oli eritasoisia lähtötietoja.

3.2 Arvioi omaa kyberturvallisuustietämystäsi luennon jälkeen.

Erittäin hyvä: 60 % (n=3). Hyvä: 40 % (n=2). Luennon jälkeen opiskelijoiden arvio omasta kyberturvallisuustietämyksestään parani huomattavasti, sillä kukaan ei arvioinut tietämystään heikoksi.

4.2 Tutkimuksen tulokset

Miten hyvin hoitohenkilökunta tuntee tietosuojaan ja kyberturvallisuuteen liittyvät periaatteet?

Tilastollista tietoa haettiin Terveyden ja hyvinvoinnin laitokselta (THL), Sotkanetistä ja Tilastokeskukselta sekä hyvinvointialueiden laadun, asiakas- ja potilasturvallisuuden raporteista. Tilastollisen tiedon etsinnässä käytettiin seuraavia hakusanoja: ”hoitohenkilökunta”, ”hoitotyö", ”koulutus”, ”kyberturvallisuus”, kyberuhat”, ”kyberuhka”,

"terveydenhuolto", ”tietojenkalastelu”, ”tietosuoja”, ”tilasto". Kävi ilmi, että Suomessa ei ollut saatavilla julkista tilastoa, joka vastaisi tutkimuskysymykseen, miten hyvin hoitohenkilökunta tuntee tietosuoja ja kyberturvallisuuteen liittyvät periaatteet.

Tietoa kysymykseen etsittiin myös hyvinvointialueiden laadun, asiakas- ja potilasturvallisuuden raporteista: Lapha (Lapin hyvinvointialue), Pirha (Pirkanmaan hyvinvointialue), Keusote (Keski-Uudenmaan hyvinvointialue), HUS (Helsingin yliopistollinen sairaala), Varha (Varsinais-Suomen hyvinvointialue), Siunsote (Pohjois-Karjalan Hyvinvointialue). Huomattiin, että myöskään hyvinvointialueiden raporteista ei löytynyt tilastoa tai tietoa vastaamaan tutkimuskysymykseen.

Vaikka Suomesta ei löytynyt tilastollista tietoa tutkimuskysymyksiin, HIPAA Journalista saatiin tietoa tietoturvaloukkauksista Yhdysvaltain terveydenhuollossa. Julkaistujen tilastojen mukaan vuonna 2023 terveydenhuoltoon kohdistui merkittävästi tietoturvaloukkauksia, yhteensä 745 tapausta ja yli 133 miljoonan tietueen paljastumista. Journalin mukaan yleisin syy tietojen vuotoon oli hakkerointi, mutta myös inhimilliset virheet, laitteiden katoaminen ja varastaminen aiheuttivat merkittäviä tietomurtoja. Nämä tiedot korostavat hoitohenkilökunnan tietoisuuden lisäämisen tärkeyttä kyberturvallisuudesta, sillä he ovat keskeisessä roolissa potilastietojen suojaamisessa ja tietoturvaloukkauksien ehkäisyssä. (Alder, 2024)

Millaisia kyberuhkia hoitohenkilökunta kohtaa päivittäisessä työssään?

Hoitohenkilökunta kohtaa päivittäisessä työssään monenlaisia kyberuhkia, joista tietojenkalastelu on kaikkein yleisin. Herjavec Groupin tutkimuksen mukaan yli 90 % terveydenhuoltoa vastaan kohdistuvista kyberhyökkäyksistä toteutuu tietojenkalasteluhuijausten muodossa. (Herjavec Group, n.d.). Tämä ilmiö on erityisen huolestuttava, sillä HIPAA Journalin mukaan 45 % terveydenhuollon kyberturvallisuuden asiantuntijoista on raportoinut, että tietojenkalasteluhyökkäys on ollut heidän organisaationsa pahin tietoturvaloukkaus. (HIPAA Journal, 2023)

Hyökkäykset voivat ilmetä eri muodoissa: yleiset sähköpostihuijaukset ovat yleisin tapa (71 %), minkä jälkeen seuraavat kohdennetut spear-phishing-hyökkäykset (67 %), äänihuijaukset (vishing) (27 %), whaling-hyökkäykset (27 %), liiketoimintaan liittyvät sähköpostihuijaukset (23 %), SMS-huijaukset (21 %), huijaussivustot (20 %), sosiaalisen median huijaukset (16 %), pharming-hyökkäykset (3 %) ja syvävääreennykset (deepfake) (2 %). Nämä uhat korostavat koulutuksen merkitystä hoitohenkilökunnan keskuudessa, jotta he pystyvät

tunnistamaan ja torjumaan näitä kyberuhkia, mikä on elintärkeää potilastietojen suojaamiseksi ja organisaatioiden kyberturvallisuuden ylläpitämiseksi. (HIPAA Journal, n.d.)

Kuinka hyvin sairaanhoitajaopiskelijat ymmärtävät kyberturvallisuuden periaatteet ja niiden soveltamisen hoitotyössä koulutuksen jälkeen?

Tutkimuksen perusteella sairaanhoitajaopiskelijat ymmärsivät kyberturvallisuuden periaatteet ja niiden soveltamisen hoitotyössä hyvin koulutuksen jälkeen. Tämä käy ilmi palautekyselystä, jossa kaikki vastaajat (100 %) olivat samaa mieltä siitä, että luennon sisältö tuki kyberturvallisuuden ymmärtämistä hoitotyön näkökulmasta. Lisäksi opiskelijoiden itsearvio omasta kyberturvallisuustietämyksestään parani huomattavasti: ennen luentoa 40 % arvioi tietämyksensä erittäin hyväksi, mutta luennon jälkeen tämä luku nousi 60 prosenttiin. Kukaan ei luennon jälkeen kokenut tietämystään heikoksi.

Miten tehokasta opetusmateriaali on opiskelijoiden kyberturvallisuusosaamisen kehittämisessä?

Opetusmateriaali osoittautui tehokkaaksi kyberturvallisuusosaamisen kehittämisessä. Palautekyselyn perusteella kaikki vastaajat (100 %) olivat sitä mieltä, että opetusmateriaalin esimerkit olivat hyödyllisiä ja tukivat oppimista. Lisäksi 80 % vastaajista koki materiaalin sisällön selkeäksi ja ymmärrettäväksi, ja loput 20 % olivat jokseenkin samaa mieltä. PowerPoint-esityksen visuaalista ilmettä pidettiin oppimista tukevana, vaikka yksi vastaaja koki, että parantamisen varaa oli jonkin verran. Näiden tulosten perusteella voidaan todeta, että opetusmateriaali oli hyvin suunniteltu ja auttoi oppimista.

Millaisia vaikutuksia koulutuksella on opiskelijoiden tietoisuuteen kyberturvallisuudesta ja sen merkityksestä hoitotyössä?

Koulutuksella oli merkittävä vaikutus opiskelijoiden tietoisuuteen kyberturvallisuudesta ja sen merkityksestä hoitotyössä. Kaikki vastaajat kokivat luennolla esitetyt asiat hyödyllisiksi kyberturvallisuuden ymmärtämisen kannalta ja 100 % vastaajista oli sitä mieltä, että luennon aikana käydyt keskustelut ja kysymykset olivat oppimista tukevia. Opiskelijoiden arvio omasta kyberturvallisuustietämyksestään parani huomattavasti luennon aikana, ja aiheen käytännönläheinen esitystapa auttoi lisäämään tietoisuutta sen merkityksestä hoitotyössä.

5 Pohdinta

Tutkimuskysymykset

Opinnäytetyön aloitusvaiheen tutkimuksessa käsiteltiin kahta keskeistä kysymystä: Miten hyvin hoitohenkilökunta tuntee tietosuojaan ja kyberturvallisuuteen liittyvät periaatteet? Millaisia kyberuhkia hoitohenkilökunta kohtaa päivittäisessä työssään? Tietojen etsimisessä hyödynnettiin useita lähteitä, kuten tilastollisia tietopankkeja, uutislähteitä ja tieteellisiä julkaisuja.

Tilastollista tietoa etsittiin tietopankeista ja hyvinvointialueiden laatu-, Terveyden ja hyvinvoinnin laitokselta (THL), Sotkanetistä ja Tilastokeskukselta, mutta havaittiin, että Suomea koskevaa julkista tilastoa, joka vastaisi tutkimuskysymyksiin, ei ollut saatavilla. Vähänkään asiaan liittyvää tietoa oli hyvin niukasti tarjolla, mikä viittasi siihen, että tutkimuskysymyksiin ei saatu kattavaa vastausta hoitohenkilöstön kyberturvallisuustietoisuudesta tai koulutuksen kohdistamistarpeista Suomen terveydenhuollossa.

Suomen tilannetta tarkasteltaessa kyberturvallisuutta koskevien tilastojen vähäisyys vaikeutti kokonaiskuvan muodostamista hoitohenkilökunnan tietosuojatietoisuudesta ja kyberuhkien kohtaamisesta työssään. Näiden tilasto- ja tutkimuslähteiden puutteet osoittavat, että aiheen kehittämiseksi Suomessa tarvittaisiin lisää resursseja ja kohdennettua tutkimusta, jotta turvallisuusriskejä voitaisiin paremmin tunnistaa ja ennaltaehkäistä. On myös mahdollista, että terveydenhuollon kyberturvallisuustilastoja ei ole julkisesti saatavilla.

Taas Yhdysvalloissa hoitohenkilökunnan kohtaamat kyberuhat, erityisesti tietojenkalastelu, korosti potilastietojen suojaamisen ja organisaatioiden kyberturvallisuuden merkitystä. Tietojenkalastelu on yleisin kyberhyökkäysmuoto terveydenhuollossa, ja kohdennetut spear-phishing hyökkäykset lisäävät tarvetta valppaudelle, henkilökunnan koulutukselle ja tehokkaille tietoturvakäytännöille.

Uutislähteet, kuten kyberturvallisuuskeskuksen julkaisut, tarjosivat tietoa ajankohtaisista kyberuhista, erityisesti tietojen kalasteluviesteistä sekä kiristysohjelmista, jotka ovat yhä merkittävä uhka terveydenhuollon henkilöstölle. Vaikka uutiset käsittelivät laajemmin kyberuhkien vaikutuksia organisaatioihin ja siviileihin, hoitohenkilökunnan altistuminen näille uhille oli vähemmän esillä uutisten julkaisu alustoilla. Tämä korostaa tiedon puutetta

aiheesta, nostattaa tarvetta kohdentaa koulutusta hoitohenkilöstölle, jotta he pystyvät tunnistamaan ja torjumaan näitä uhkia.

Opetusmateriaali

Teoreettisen viitekehyksen pohjalta laadittiin opetusmateriaali sairaanhoitajaopiskelijoille, hyödyntäen laajasti saatavilla olevaa tietoa kyberturvallisuudesta. Koska hoitohenkilökunnalle suunnattuja julkisia kyberturvallisuusohjeistuksia ja koulutuksia on rajatusti saatavilla internetissä, opetusmateriaalissa jouduttiin soveltamaan myös yleisiä tietoturvan ja kyberturvallisuuden periaatteita. Materiaalia valmistettaessa otettiin huomioon ajankohtaiset kyberturvallisuusuhat, joita on havaittu terveydenhuollon sektorilla. Käytännön suojautumiskeinoissa ja raportoinnissa hyödynnettiin osittain hyvinvointialueiden, kuten Pohjois-Karjalan hyvinvointialueen, antamia ohjeita.

Pirkanmaan hyvinvointialueelta pyydettiin erityisiä kyberturvallisuusohjeita hoitohenkilökunnalle, mutta näitä ei annettu julkiseen käyttöön. Sen sijaan tarjottiin linkkejä julkisesti saatavilla oleviin resursseihin, joiden pohjalta osa heidän sisäisistä ohjeistuksistaan on laadittu. Alue perusteli päätöstään sillä, että heidän sisäiset ohjeensa on tarkoitettu vain henkilöstön käyttöön, koska ne voivat sisältää arkaluonteista tietoa, jonka jakaminen voisi aiheuttaa kyberturvallisuusriskin. Koska hyvinvointialueiden käytännöt ja koulutukset eroavat toisistaan, ei ollut mahdollista laatia täysin yhtenäistä ohjeistusta. Tästä syystä opetusmateriaalissa jouduttiin tukeutumaan julkisesti saatavilla oleviin lähteisiin, mikä vaikutti osaltaan materiaalin sisältöön ja rakenteeseen.

Opetusmateriaalissa ei kerrottu laajemmin tekoälyn käytöstä kyberrikollisuudessa, koska tietoa tekoälyn haitallisesta käytöstä terveydenhuollossa ei löydetty hoito henkilökuntaan liittyviä tapauksia internetistä. Kuitenkin tiedetään, että terveydenhuoltoon kohdistuvissa kyberhyökkäyksissä voidaan hyödyntää tekoälyä esimerkiksi tietojen kalastelun, kiristysohjelmien ja syvä väärennöksen (deepfake) yhteydessä.

Luento ja palaute

Luennon ja palautteen pohjalta voidaan todeta, että kyberturvallisuuskoulutus oli onnistunut ja saavutti sille asetetut tavoitteet. Luento tarjosi sairaanhoitajaopiskelijoille selkeän ja ymmärrettävän katsauksen kyberturvallisuuden periaatteista sekä niiden merkityksestä hoitotyössä. Palautekyselyn tulokset osoittavat, että opiskelijat kokivat opetusmateriaalin ja luennon yleisesti hyvin onnistuneiksi. Yksittäiset palautevastaukset vahvistavat, että koulutus

lisäsi opiskelijoiden tietämystä ja ymmärrystä kyberturvallisuudesta, mikä on tärkeä osa nykypäivän hoitotyötä.

On kuitenkin syytä huomioida, että vastaajien määrä oli pieni (vain 5 henkilöä), mikä rajoitti palautteen yleistettävyyttä. Pienellä vastaajaryhmällä ei voida täysin arvioida koko monimuotototeutuksen opiskelijaryhmän kokemuksia ja mielipiteitä. On mahdollista, että suuremmassa ryhmässä ilmenevät mielipiteet ja kokemukset voisivat olla hieman erilaisia. Jatkossa voisi olla hyödyllistä kerätä palautetta laajemmalta osallistujajoukolta, jolloin palautteen perusteella voisi tehdä tarkempia johtopäätöksiä koulutuksen vaikuttavuudesta ja hyödyllisyydestä.

Tulevaisuuden kehitysehdotukset

Vaikka koulutus oli pääsääntöisesti onnistunut, palautteen perusteella olisi hyödyllistä kehittää luentomateriaalia ja koulutustapaa edelleen. Esimerkiksi visuaalisen ilmeen parantaminen voisi olla yksi kehitettävä alue, erityisesti jos se voisi tukea oppimisprosessia entistä tehokkaammin. Myös käytännön esimerkkejä voisi tuoda enemmän esille kerrottaessaan kyberuhkien vaikutuksista hoitotyöhön. Luennolla tuli kysymyksiä liittyen potilastietojen luovuttamiseen potilaan siirtyessään toiseen yksikköön jatkohoitoon tilanteessa, jossa yksiköiden välissä on eri potilastietojärjestelmät. Tähän kysymykseen pohdittiin vastausta ja käytiin läpi paperisen potilasasiakirjan luovuttamisen riskejä potilasturvallisuuden ja tietoturvallisuuden näkökulmasta. Tämän aiheen kysymyksestä voisi lisätä tietoa materiaaliin.

Lisäksi interaktiivisuutta voisi lisätä entisestään, jolloin opiskelijat voisivat osallistua vielä aktiivisemmin keskusteluihin ja pohdintoihin. Erityisesti käytännön harjoitusten lisääminen voisi parantaa kyberturvallisuuden soveltamista hoitotyöhön. Koulutuksen pituus ja syvyys voivat myös olla tärkeitä tekijöitä luennon tehokkuuden kannalta. Kyberturvallisuus on laaja ja monivaiheinen aihe, joka saattaa vaatia useampia koulutustilaisuuksia. Tämä voisi tarjota opiskelijoille mahdollisuuden syventää ymmärrystään ja soveltaa oppimaansa pidemmällä aikavälillä.

Lähteet

Alder, S. (2024*). Healthcare Data Breach Statistics*. The HIPAA Journal.
https://www.hipaajournal.com/healthcare-data-breach-statistics/

Massive ransomware infection hits computers in 99 countries. (13.5.2017). *BBC.*
https://www.bbc.com/news/technology-39901382

Bowcut, S. (2023). *Protecting patient data: Cybersecurity in the healthcare industry. Cybersecurity Guide.*
https://cybersecurityguide.org/industries/healthcare/

Cybersecurity for the Clinician - *Episode 6: Tips for Protection*. (2023). [Video]. Youtube.
https://www.youtube.com/watch?v=5l04KcuWg70&ab_channel=HealthcareCybersecurity

Digi- ja väestötietovirasto. (2024). *Sosiaali- ja terveydenhuollon ammattikortti*.
https://dvv.fi/sote-ammattikortti

F-Secure. (2024a). *Mikä on VPN?*
https://www.f-secure.com/fi/articles/what-is-a-vpn

F-Secure. (2024b). *Mitä on kohdennettu tietojen-kalastelu eli spear phishing?*
https://www.f-secure.com/fi/articles/spear-phishing

F-Secure. (2024c). *Mitä on kyberturvallisuus?*
https://www.f-secure.com/fi/articles/what-is-cyber-security

F-secure. (2024d). *Strong password generator*.
https://www.f-secure.com/en/password-generator

HaiPro. (2019). *Potilasturvallisuusilmoituksen täyttöohje*.
https://awanic.fi/haipro/#tutkijoille

Healthcare Cybersecurity. (5.4.2023). *Cybersecurity for the Clinician - Episode 1: Cyber Safety Is Patient Safety* [video]. YouTube. https://www.youtube.com/watch?v=rS0gT6bIiYw&ab_channel=HealthcareCybersecurity

Helsingin yliopisto. (2024). *Tiedostojen varmuuskopiointi.* https://blogs.helsinki.fi/opiskelijan-digitaidot/4-tietoturva/4-2-suojautuminen-uhkatekijoilta/tiedostojen-varmuuskopiointi/

Herjavec Group. (n.d.). *Healthcare Cybersecurity Report 2021-2022*. https://www.herjavecgroup.com/?s=cybersecurity+report

Hive systems. (2024). *Are your passwords in the green?* https://www.hivesystems.com/blog/are-your-passwords-in-the-green

HIPAA Journal. (n.d.). *State of Healthcare Cybersecurity*. https://www.hipaajournal.com/healthcare-cybersecurity/

Hämäläinen, V. (22.1.2021). Uudet tiedot: Vastaamon potilaiden tiedot olivat ehkä jopa vuosia suojaamatta netissä – tietoturva-asiantuntija: "Älyvapaata". *Yle*. https://yle.fi/a/3-11750220

IBM Technology. (2.5.2023). *Security Operations Center (SOC) Explained* [Video]. YouTube. https://www.youtube.com/watch?v=OHkWXFheSKM&ab_channel=IBMTechnology

Vertainen, V., Suni, E., Vatanen, M., Hautamäki, J., Laava, T & Piispanen, J. (2024).*Kyberhäiriöiden hallinta – Käsikirja terveydenhuollon toimijoille*. Jyvsectec. https://jyvsectec.fi/2021/01/kyberhairioiden-hallinta-kasikirja-terveydenhuollon-toimijoille/

Keusote. (2024). *Laadun, asiakas- ja potilasturvallisuuden raportti 2023*. https://www.keusote.fi/etusivu/meilla-asiakkaana/laatu/laadun-ja-omavalvonnan-raportointi/

Keränen, T. (2017). *WannaCry-haittaohjelma löytyi TYKS:stä*. Lääkärilehti. https://www.laakarilehti.fi/ajassa/ajankohtaista/wannacry-haittaohjelma-loytyi-tyks-sta/

Kyberturvallisuuskomitea (2017). *Kodin kyberopas. – ohjeita digitaaliseen arkeen*. https://turvallisuuskomitea.fi/viestinta/julkaisut/

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 784/2021. https://www.finlex.fi/fi/laki/alkup/2023/20230703

Microsoft. (2024a). *Auta suojaamaan Outlook.com-sähköpostitilisi*. https://support.microsoft.com/fi-fi/office/auta-suojaamaan-outlook-com-s%C3%A4hk%C3%B6postitilisi-a4f20fc5-4307-4ece-8231-6d4d4bd8a9ba

Microsoft. (2024b). *Create and use strong passwords*. https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb

Microsoft. (2024c). *Mitä on tietojenkalastelu?* https://www.microsoft.com/fi-fi/security/business/security-101/what-is-phishing

Microsoft. (2024d). *Mitä tietoturva on?* https://www.microsoft.com/fi-fi/security/business/security-101/what-is-data-security

Microsoft. (2024e). *VPN-yhteyden muodostaminen Windowsissa*. https://support.microsoft.com/fi-fi/windows/vpn-yhteyden-muodostaminen-windowsissa-3d29aeb1-f497-f6b7-7633-115722c1009c

Microsoft. (2024f). *What is ransomware?* https://learn.microsoft.com/en-us/security/ransomware/human-operated-ransomware

Norja, S., Kellomäki, T., Nykänen, R., Vepsäläinen, P. & Radi, H. (2024). *Tietoturva sosiaali- ja terveydenhuollossa*. Duodecim oppiportti verkkokurssit. https://www.oppiportti.fi/dvk00150

Ontrack. (2022). *Kuinka vältät kiristysohjelmia tänä päivänä?* https://www.ontrack.com/fi-fi/blog/kuinka-valtat-kiristysohjelmia-tana-paivana

Pirha. (2024). *Henkilötietojen tietoturvaloukkaus*. https://www.pirha.fi/henkilotietojen-tietoturvaloukkaus

Rautio, M. (3.6.2017). Kelan Kanta-palvelut vaikeuksissa – syynä jälleen palvelunestohyökkäys. *Yle*.
https://yle.fi/a/3-9647957

Sairaanhoitajat. (2021). *Digitaaliset taidot osana sairaanhoitajan työtä*.
https://sairaanhoitajat.fi/ammatti-ja-osaaminen/digitaaliset-taidot-osana-sairaanhoitajan-tyota/

Simplilearn. (2024). *20 Emerging Cybersecurity Trends to Watch Out in 2024*.
https://www.simplilearn.com/top-cybersecurity-trends-article

Siun SOTE. (2024). *Toimintaohje: Tietosuoja- ja tietoturvakäsikirja*.
https://www.siunsote.fi/sosiaali-ja-terveysala?inheritRedirect=true

Sonic wall. (2023). 2023 *Sonic wall cyber threat report*.
https://www.sonicwall.com/resources/white-papers/2023-sonicwall-cyber-threat-report/gated/thank-you/asset

STM. (2019). *Ohje sosiaali- ja terveydenhuollon toimijoille*.
https://julkaisut.valtioneuvosto.fi/handle/10024/161683

THL. (2024a). *Kirjaaminen*.
https://thl.fi/aiheet/tiedonhallinta-sosiaali-ja-terveysalalla/kirjaaminen

THL. (2024b). *Opas sosiaali- ja asiakastietojen käsittelystä täydentää kirjaamisen kokonaisuutta*.
https://thl.fi/-/opas-sosiaali-ja-asiakastietojen-kasittelysta-taydentaa-kirjaamisen-kokonaisuutta

Tietosuojakeskus. (n.d.). *Case Vastaamo*.
https://tietosuojakeskus.fi/case-vastaamo/

Tietosuojavaltuutetun toimisto. (2024). *Tietoturvaloukkaukset.*
https://tietosuoja.fi/tietoturvaloukkaukset

Traficom. (2020a). *Pienyritysten kyberturvallisuusopas*.
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/uusi-oppaamme-auttaa-vahvistamaan-pienyritysten-kyberturvallisuutta

Traficom. (2020b). *SolarWinds Orion Platformin takaovi mahdollisti vakoilun ja tietomurtoja*.
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/solarwinds-orion-platformin-takaovi-mahdollisti-vakoilun-ja-tietomurtoja

Traficom. (2022a).*Toiminta kiristyshaittaohjelmatilanteessa - johdon ohje*.
https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/toiminta-kiristyshaittaohjelmatilanteessa-johdon-ohje

Traficom. (2022b). *Toimintaohje – Tietomurto*.
https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/toimintaohje-tietomurto

Traficom. (2023). *Turvapostiteemaiset kalasteluviestit johtavat sähköpostitilimurtoihin*.
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/turvapostiteemaiset-kalasteluviestit-johtavat-sahkopostitilimurtoihin

Traficom. (2024a). *Kun jokainen päivä voi olla aprillipäivä - Mistä deepfakeissa on kysymys?*
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kun-jokainen-paiva-voi-olla-aprillipaiva-mista-deepfakeissa-kysymys

Traficom. (2024b). *Kybersää*.
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa?toggle=Kybers%C3%A4%C3%A4tiedotteet%202024

Traficom. (2024c). *Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi*.
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi

Traficom. (2024d). *Tekoälyn mahdollistamat kyberhyökkäykset*.
https://traficom.fi/fi/julkaisut/tekoalyn-mahdollistamat-kyberhyokkaykset

Liite 1. PowerPoint esitys kyberturvallisuus hoitotyössä

Kyberturvallisuus hoitotyössä

Tarkoitus ja tavoitteet

Tämän luennon tarkoituksena on vahvistaa sairaanhoitaja opiskelijoiden tietoturvaosaamista ja lisätä heidän tietoisuuttaan kyberturvallisuuden merkityksestä terveydenhuollossa.

Tavoitteena on, että opiskelijat ymmärtävät selkeästi kyberturvallisuuden merkityksen hoitotyössä ja saavat käytännön valmiuksia tunnistaa tietoturvauhkia sekä suojata arkaluonteisia tietoja, kuten potilastietoja.

Tämän luennon jälkeen:

- Tiedät mikä on kyberturvallisuuden merkitys terveydenhuollossa
- Tunnistat yleisiä kyberuhkia, joita saatat kohdata töissä tai arkielämässäsi
- Osaat toimia ja suojautua kyberuhilta


Termistö
• Tietoturvallisuus tarkoittaa sitä, että sinun tietojasi voi käyttää ja muuttaa sinun lisäksesi vain siihen erikseen oikeutetut tahot.
• Tietomurto tarkoittaa luvattoman pääsyn hankkimista tietojärjestelmään, palveluun tai laitteeseen, usein hyödyntämällä varastettuja tunnuksia. Tietomurron tavoitteena on yleensä taloudellinen hyöty, esimerkiksi varastamalla myytäväksi kelpaavia tietoja.
• Tietoturva tarkoittaa tiedon suojaamista sen saatavuuden, luottamuksellisuuden ja eheyden varmistamiseksi. Tämä koskee niin digitaalisia kuin fyysisiä tallenteita sekä työntekijöiden tietämystä. Tietoturva on tärkeää myös tiedon siirron aikana.
• Tietoturvaloukkaus on tapahtuma, jossa henkilötiedot vaarantuvat esimerkiksi tuhoutumalla, häviämällä, muuttumalla tai päätyessä luvattomasti vääriin käsiin. Se voi johtua esimerkiksi laitteiden katoamisesta, hakkeroinnista, kyberhyökkäyksestä tai virheellisestä tietojen käsittelystä.


Termistö
• Tietue on tietokokonaisuus, joka sisältää yhteen henkilöön, tapahtumaan tai asiaan liittyviä tietoja, kuten esimerkiksi henkilön nimi ja syntymäpäivä. Tietojenkäsittelyssä se on yhdistelmä toisiinsa liittyviä tietoja. Tiedonhallinnassa tietue muodostaa yhden kohteen tiedot, kuten asiakasrekisterissä yhden asiakkaan tiedot.
• Takaovi on ohjelmistoon tahallaan tai vahingossa jätetty piilotettu reitti, jonka kautta järjestelmään voi päästä ohi normaalien turvamekanismien. Hyökkääjät voivat käyttää takaovia järjestelmän hallintaan, tietojen varastamiseen tai lisähyökkäysten valmisteluun.
• SOC (Security Operations Center) on tietoturvakeskus, joka valvoo organisaation tietoverkkoa, havaitsee uhkia ja reagoi niihin suojatakseen järjestelmiä kyberhyökkäyksiltä.

Sisällysluettelo

1. Johdanto kyberturvallisuuteen hoitotyössä
2. Kyberhyökkäykset terveydenhuollossa
3. Sairaanhoitajan rooli kyberturvallisuudessa
4. Kyberhyökkäysmetodeja terveydenhuollossa
5. Käytännön keinot suojautua hoitotyössä
6. Kyberuhkien ilmoittaminen hoitotyössä
7. Potilastietojen käsittely ja suojaaminen

1. Johdanto kyberturvallisuuteen hoitotyössä

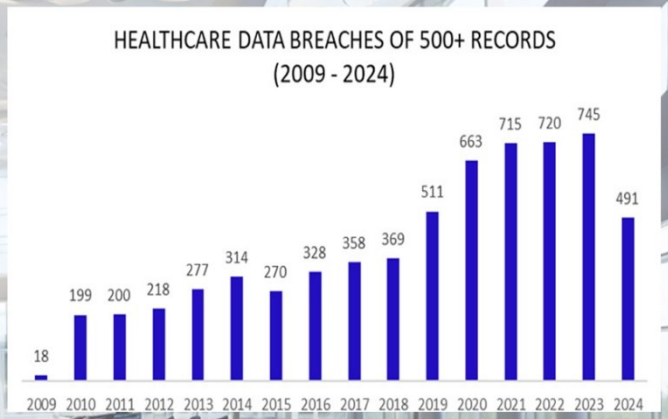
- **Kyberturvallisuus** tarkoittaa tietojen ja järjestelmien suojaamista
- Terveydenhuollossa tietojen ja järjestelmien suojaaminen on kriittistä potilasturvallisuuden ja organisaation toiminnan turvaamiseksi
- Terveydenhuollossa suojattavia tietoja ovat potilastiedot, hoitohenkilökunnan tiedot, lääketieteellisten laitteiden tiedot sekä järjestelmien ja verkkoinfrastruktuurin tiedot

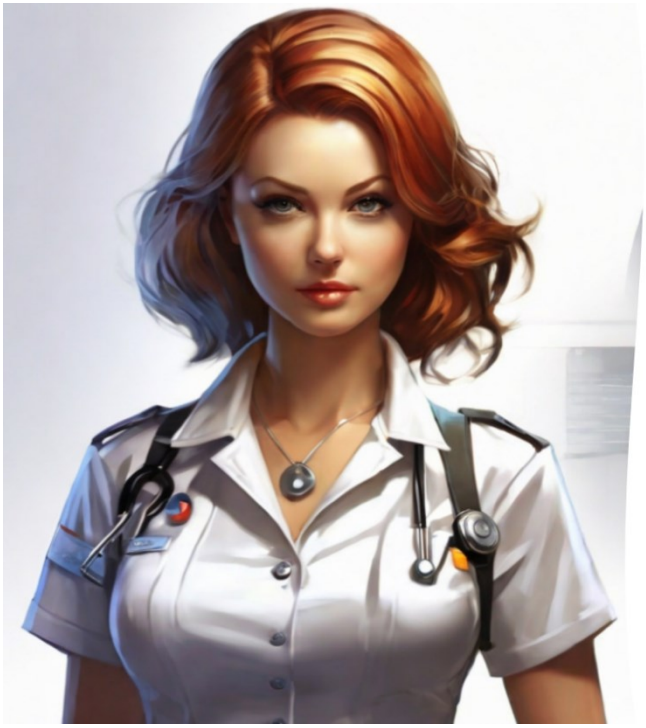
1. Johdanto kyberturvallisuuteen hoitotyössä

- **Terveydenhuollon erityiset haavoittuvuudet kyberuhkien näkökulmasta**
  - tietomurrot & kiristyshaittaohjelmat
  - IoT-laitteet (tietokoneet, puhelimet, lääkinnälliset laitteet jne.)
  - terveydenhuollon toimintaympäristö
  - inhimilliset virheet
- **Kyberuhkien vaikutukset potilasturvallisuuteen, luottamukseen ja organisaation toimintaan**
  - Tietovuodot ja kyberhyökkäykset voivat johtaa potilaiden tietojen väärinkäyttöön, hoitovirheisiin ja taloudellisiin tappioihin
  - Epäonnisteen kyberturvallisuuden seurauksena luottamus organisaatioon voi heikentyä

2. Kyberhyökkäykset terveydenhuollossa

- USA:ssa terveydenhuollon tietomurtojen määrä on kasvanut huomattavasti vuosien varrella
- Hakkerointi on yleisin syy terveydenhuollon tietomurtoihin
- Vuonna 2023 ilmoitettiin 725 tietoturvaloukkauksesta, joissa paljastui tai vuoti luvattomasti yli 133 miljoonaa potilastietuetta





3. Sairaanhoitajan rooli kyberturvallisuudessa

Mitä tietoja sairaanhoitaja käsittelee?

- Sähköposteja
- Potilastietoja
- Lääkinnällisiä laitteita paikallisesti ja langattomasti
- Yksityissektorilla myös asiakasmaksuja

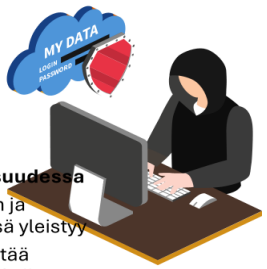
Mikä on sairaanhoitajan vastuu?

- Tietojen oikeanlainen käsittely ja varmistaminen, että vain valtuutetut henkilöt pääsevät niihin käsiksi
- Tietoturvakäytäntöjen noudattaminen ja kyberuhkien tunnistaminen sekä ilmoittaminen

Et ole yksin organisaatiosi kyberturvallisuuden turvaamisessa. Sinun tukenasi on:

- Tietoturvavalvomo (Security operations center, SOC)
- IT-osasto (Ohjelmisto- ja järjestelmä kehitys sekä päivitykset)
- Käyttäjätuki (Tietokone ja laite asiat sekä potilastietojärjestelmät)

4. Kyberhyökkäysmetodeja terveydenhuollossa



Top 5 kyberuhat tulevaisuudessa

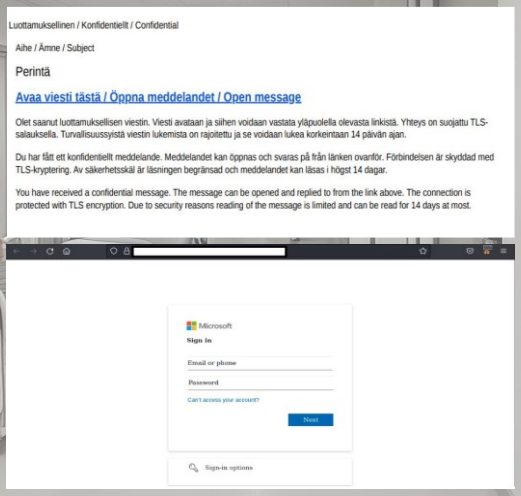
- **Haavoittuvuuksien nopeampi hyödyntäminen**
  - Rikolliset hyödyntävät haavoittuvuuksia heti niiden julkistamisen jälkeen
  - Takaovien luominen järjestelmiin on yleistä
  - Järjestelmien nopea päivittäminen on kriittistä
- **Kiristyshaittaohjelmat**
  - Kiristyshaittaohjelmat (esim. Akira ja Wannacry) uhkaavat terveydenhuoltoa.
  - Double extortion -taktiikka: tiedostojen salaus + tietojen varastaminen.
- **Toimitus- ja Palveluketjujen Haavoittuvuudet**
  - Ulkopuoliset toimittajat voivat olla tietoturvauhka
  - Toimitusketjujen turvallisuuden ymmärtäminen on elintärkeää
- **Tekoäly Perinteisessä Kyberrikollisuudessa**
  - Tekoälyn käyttö haittaohjelmien ja kalasteluviestien kehittämisessä yleistyy
  - Syväväärennöksiä voidaan käyttää identiteettivarkauksiin ja huijauksiin
- **Tietoliikenneinfran Suojaus**
  - Tietoliikenneinfran fyysinen ja digitaalinen suojaus on kriittistä
  - Luonnonilmiöiden ja hyökkäysten vaikutukset tietoliikenneinfraan voivat olla merkittäviä

4. Kyberhyökkäysmetodeja terveydenhuollossa

- **Tietojen kalastelu Phishing**
- Petosmenetelmä, jossa huijari yrittää kalastella henkilökohtaisia tietoja tekeytymällä luotettavaksi tahoksi sähköisessä viestinnässä
- **Miten tunnistaa phishing-viestit**?
  - Viestissä on kirjoitusvirheitä tai epäloogisia lauseita
  - Viestissä pyydetään henkilökohtaisia tietoja (esim. salasana tai luottokortin numero)
  - Viesti luo kiireellisyyden tunteen (Uhkailu tilin sulkemisella)
  - Linkin URL-osoite eroaa odotetusta
  - Epäilyttävä lähettäjän sähköpostiosoite tai suuntanumero
- **Estämiskeinot ja toimintatavat**
  - Ole skeptinen odottamattomista viesteistä
  - Tarkista viestin aitous organisaation virallisilta kanavilta
  - Käytä kaksivaiheista tunnistautumista
  - Pidä ohjelmistot ja virustorjunta ajan tasalla
  - Älä klikkaa epäilyttäviä linkkejä tai avaa tuntemattomia liitteitä

4. Kyberhyökkäysmetodeja terveydenhuollossa

- **Kohdistettu tietojen kalastelu Spear Phishing**
- Kohdennettu tietojenkalastelu, jossa hyökkäys suunnataan tarkasti valittuun henkilöön tai organisaatioon
- **Miten tunnistaa spear phishing-viestit?**
  - Personoidut viestit, joissa on tarkkoja tietoja
  - Yllättävät ja kiireelliset pyynnöt
  - Lähettäjän osoitteessa pieniä epäilyttäviä virheitä **juuso.mantymaki@meh1läinen.com**)
  - Virheellinen konteksti, esim. väärät nimet tai ajankohdat
- **Estämisen keinot ja toimintatavat**
  - Tarkista lähettäjän henkilöllisyys
  - Älä klikkaa linkkiä tai jaa luottamuksellista tietoa
  - Käytä kaksivaiheista tunnistautumista
  - Ilmoita huijausviestistä
- Oikealla esimerkki organisaatioon kohdistetusta



4. Kyberhyökkäysmetodeja terveydenhuollossa

- **Kiristysohjelma Ransomware**
- Terveydenhuollossa kyberrikollinen käyttää kiristysohjelmia salaamaan tai sekoittamaan potilastietoja, aikatauluja ja maksujärjestelmiä, vaatien lunnaita tietojen palauttamiseksi
- **Kuinka tunnistaa kiristysohjelma?**
  - Tiedostojen äkillinen salautuminen
  - Lunnasviesti
  - Tavalliset kiristysohjelman merkit: kysymykset tiedostojen lukitsemisesta, uusien tiedostojen luomisesta
- **Estämisen keinot ja toimintatavat?**
  - Säännöllinen varmuuskopiointi
  - Päivitykset ja korjaustiedostot
  - Vahva verkkoturvallisuus
  - Käyttöoikeuksien rajoittaminen
  - Älä maksa lunnaita!

5. Käytännön keinot suojautua hoitotyössä

Salasanat

- Vahva salasana on
  - Vähintään 12 merkkiä pitkä (suositus)
  - Sisältää isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä.
  - Ei ole sanakirjasana tai henkilö- tai tuotteen nimi
  - Erottuu merkittävästi aikaisemmista salasanoista
  - Helppo muistaa mutta vaikea arvata. Esimerkiksi: **5BlueGiraffes@Jump!**

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

Hardware: 12 x RTX 4090 | Password hash: bcrypt

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

5. Käytännön keinot suojautua hoitotyössä

Ohje sähköpostin turvalliseen käyttöön

- Sähköpostikirjautuminen
  - **Vahva salasana**
  - **Kaksivaiheinen kirjautuminen:** esimerkiksi tekstiviestitse, puhelulla tai todennussovelluksella tapahtuva todennus
- Vältä epäilyttävien linkkien avaamista
  - **Tarkasta lähettäjän osoite:** Älä luota pelkkään nimeen, vaan vie hiiri osoitteen päälle nähdäksesi, mistä viesti on todella lähetetty.
  - **Älä avaa tuntemattomia liitteitä:** Varo erityisesti tiedostoja, joilla on epäilyttäviä päätteitä (.exe, .vbs, .com). Varmista, että liite on luotettavalta lähettäjältä.
  - **Älä klikkaa linkkejä suoraan:** Tarkasta linkin osoite viemällä hiiri sen päälle. Varmista, että linkki johtaa oikealle sivustolle.

5. Käytännön keinot suojautua hoitotyössä

Ohjeet tietokoneen turvalliseen käyttämiseen

- **Lukitse työasema aina poistuessasi senääreltä potilasturvallisuuden ja tietosuojan varmistamiseksi**
  - Työasemaa ei saa koskaan jättää valvomattomana auki
  - Tiesitkö, että voit lukita työaseman nopeasti painamalla Windows-näppäintä ja L-kirjainta samanaikaisesti
- **Pidä tietokoneesi päivitykset aina ajan tasalla**, jotta järjestelmäsi pysyy suojattuna uusimmilta turvallisuusuhkilta
- **Käytä etätyöskentelyssä VPN-yhteyttä**
  - VPN yhteys suojaa arkaluonteisia potilastietoja tiedonsiirron aikana
  - Etätyössä VPN mahdollistaa turvallisemman pääsyn terveydenhuollon järjestelmiin
  - **VPN-yhteyden voi tunnistaa kahdella tavalla:**
    - VPN-asetuksista: Yhdistetyn VPN-yhteyden nimi näkyy asetussivulla.
    - Tehtäväpalkin kuvakkeesta: Sininen kilpi ilmestyy tehtäväpalkkiin, kun VPN on aktiivinen

- **Varmuuskopio tärkeimmät tietosi**
  - Älä kuitenkaan varmuuskopioi tai tallenna tietojasi verkkopalveluun, jota IT-osastosi ei ole hyväksynyt

5. Käytännön keinot suojautua hoitotyössä

Kaksivaiheinen tunnistautuminen varmennekortilla

Varmennekortti (toimikortti, Sote ammattikortti)

- Toimikortti on henkilökohtainen ja sen käytöstä vastaa kortinhaltija
- Kortti on säilytettävä huolellisesti ja erillään tunnusluvuista
- Vahingoittuneesta, kadonneesta tai tarpeettomasta kortista on ilmoitettava välittömästi **varmennekorttien sulkupalveluun** väärinkäytösten estämiseksi.
- Kortin numero kannattaa tallentaa sulkemista varten
- Lisätietoa https://dvv.fi/sote-ammattikortti

6. Kyberuhkien raportointi hoitotyössä

Toimi näin, jos epäilet olevasi kyberuhan kohteena

- Noudata organisaatiosi toimintasuunnitelmaa
- Älä avaa epäilyttäviä tiedostoja, linkkejä tai vaarantuneita järjestelmiä
- Älä vastaa viestiin tai anna mitään henkilökohtaisia tietoja, kuten salasanoja, henkilötunnuksia tai pankkitietoja

- Ilmoittaminen
  - **Ota yhteyttä oman työpaikkasi käyttötukeen (helpdesk) ja kerro epäilyksestäsi**
  - **Ilmoita esihenkilöllesi tietoturvahäiriöstä:** Näin varmistetaan tiedonkulku ja sovitaan mahdollisista jatkotoimenpiteistä, kuten HaiPro-ilmoituksen tekemisestä/käsittelystä.
  - **Anna kaikki tarvittavat tiedot:**
    - Jos kyseessä on kalastelu-viesti anna: Viestin lähettäjän tiedot (numero tai sähköpostiosoite). Viestin sisältö (liitä mukaan mahdolliset kuvakaappaukset).
    - Mikäli ilmoitat järjestelmästä tai laitteesta, ilmoita häiriön tyyppi (esim. tietojärjestelmän toimimattomuus, tietojen väärinkäyttö, laitevika)
    - Lisää tarvittaessa myös kuvakaappaus ja mihin järjestelmään tai laitteeseen häiriö liittyy sekä häiriön tarkka ajankohta ja vaikutukset

- Ilmoituksen jälkeen
  - Kun häiriö on ilmoitettu, järjestelmän omistaja tai tietohallinto analysoi tilannetta tarkemmin. Jos epäillään kyberuhkaa, voidaan varmistaa, että kyseessä on todellinen tietoturvaloukkaus.
  - Saat ilmoituksen aikana ja jälkeen ohjeistuksen


6. Kyberuhkien raportointi hoitotyössä
ilmoitettavia tietosuojapoikkeamia ovat:
• Henkilötietoja sisältävien aineistojen katoaminen
• Potilas-, asiakas-, henkilöstö- tai yhteystietoja sisältävien tiedostojen tai dokumenttien katoaminen.
• Muistitikkujen tai tallennusvälineiden katoaminen
• Muistitikkujen, ulkoisten kovalevyjen tai muiden tallennusvälineiden, jotka sisältävät henkilötietoja, katoaminen.
• Työaseman varastaminen
• Työaseman, läppärin tai muun laitteen, joka sisältää henkilötietoja, varastaminen.
• Henkilötietoja sisältävien asiakirjojen tai tulosteiden löytäminen väärästä paikasta
• Asiakirjoja, jotka sisältävät henkilötietoja, löytyy julkisista tai valvomattomista tiloista.
• Henkilötietojen vahingossa julkistaminen verkkosivustolla
• Henkilötietoja sisältävien dokumenttien tulostaminen ja niiden päätyminen vahingossa julkiseen verkkosivustoon intranetin sijaan.
• Dokumenttien tulostaminen väärälle tulostimelle
• Henkilötietoja sisältävien dokumenttien tulostaminen väärälle tulostimelle ja näiden dokumenttien katoaminen tai löytymättä jääminen.
• Muut tietosuojapoikkeamat
• Tilanteet, joissa epäilet tietosuojan vaarantuneen tai vaativan toimenpiteitä.


7. Potilastietojen käsittely ja suojaaminen
Potilastietojen kirjaaminen
• Potilastietojen kirjaaminen on oleellinen osa hoitotyötä, ja sillä varmistetaan hoidon jatkuvuus ja laatu
• Potilastietojen kirjaaminen tulee tehdä huolellisesti ja tarkasti, noudattaen voimassa olevia lakeja ja organisaation ohjeistuksia
• Kirjauksissa on varmistettava, että vain tarpeellinen tieto tallennetaan. Tiedon on oltava ajantasainen ja luotettava
• Tiedot kirjataan viipymättä tai heti kun mahdollista hoitotoimenpiteen tai tapahtuman jälkeen
• Kirjausten tulee olla täsmällisiä, selkeitä ja loogisia. Potilastietojen on oltava helposti ymmärrettäviä sekä muille hoitohenkilökunnan jäsenille että potilaalle itselleen
• Potilaan tietoihin tulee kirjata vain tarkastettuja ja varmoja tietoja. Epävarmat tiedot on merkittävä selvästi
• Sosiaalisessa mediassa toimiessasi muista aina suojata potilaiden yksityisyys, noudattaa salassapitovelvollisuutta ja erottaa ammatillinen ja henkilökohtainen some-käyttö.
• Muista, että työvälineet ja työaika on tarkoitettu vain työtehtäviin. Sosiaalisen median käyttö on sallittua ainoastaan, jos se liittyy suoraan työtehtäviisi.


7. Potilastietojen käsittely ja suojaaminen
Potilastietojen käsittely
• Potilastiedot ovat arkaluonteisia ja niiden suojaaminen on kriittistä tietoturvan kannalta
• Sairaanhoitajilla on velvollisuus varmistaa, että:
• Tietojärjestelmät, joissa potilastietoja käsitellään, ovat turvallisia ja niiden käyttö on suojattu omalla henkilökohtaisella käyttäjätunnuksella ja salasanalla
• Tietoja ei jaeta muille kuin hoitoon osallistuville henkilöille
• Väärinkäytöksistä ilmoitetaan välittömästi tietoturvasta vastaavalle taholle


7. Potilastietojen käsittely ja suojaaminen
Potilastietojen luovuttaminen
• Potilastietoja saa luovuttaa vain potilaan suostumuksella tai lain perusteella
• Potilas voi tarkastella Kanta-palveluun tallennettuja tietojaan OmaKannasta, mikä vähentää erillisten tietopyyntöjen tarvetta
• Luovuttaja on vastuussa tietojen lainmukaisesta luovuttamisesta ja voi pyytää pyytäjältä lisätietoja tarkoituksesta sekä lain perusteesta ennen luovutusta
• Lailliselle edustajalle tai läheiselle tiedon luovuttaminen
• Lailliselle edustajalle tai läheiselle voidaan antaa tietoa potilaan terveydentilasta, jos potilas ei pysty päättämään hoidostaan, eikä ole syytä olettaa, että hän kieltäisi tietojen antamisen.
• Laillinen edustaja tai läheinen saa tarpeelliset tiedot hoitopäätöksen tekemistä varten
• Kaikki tietojen luovutukset kirjataan potilastietojärjestelmään

Lähteet

- Alder, S. (2024). Healthcare Data Breach Statistics. The HIPAA Journal. https://www.hipaajournal.com/healthcare-data-breach-statistics/
- Cybersecurity Guide. (2024). Protecting patient data: Cybersecurity in the healthcare industry. https://cybersecurityguide.org/industries/healthcare/
- Cybersecurity for the Clinician - Episode 6: Tips For Protection. (2023). [Video] (https://www.youtube.com/watch?v=5l04KouWg70&ab_channel=HealthcareCybersecurity
- Digi- ja väestötietovirasto. (2024). Sosiaali- ja terveydenhuollon ammattikortti. https://dvv.fi/sote-ammattikortti
- F-Secure. (2024). Mikä on VPN? https://www.f-secure.com/fi/articles/what-is-a-vpn
- F-Secure. (2024). Mitä on kohdennettu tietojenkalastelu eli spear phishing? https://www.f-secure.com/fi/articles/spear-phishing
- F-secure. (2024). Mitä on kyberturvallisuus? https://www.f-secure.com/fi/articles/what-is-cyber-security
- F-secure. (2024). Strong password generator. https://www.f-secure.com/en/password-generator
- HaiPro. (2019). Potilasturvallisuusilmoituksen täyttöohje. https://awanic.fi/haipro/#tutkijoille
- Healthcare Cybersecurity. (5.4.2023). Cybersecurity for the Clinician - Episode 1: Cyber Safety Is Patient Safety [video]. YouTube. https://www.youtube.com/watch?v=rS0gT6b[illegible]&ab_channel=HealthcareCybersecurity

Lähteet

- Helsingin yliopisto. (2024). Tiedostojen varmuuskopiointi. https://blogs.helsinki.fi/opiskelijan-digitaidot/4-tietoturva/4-2-suojautuminen-uhkatekijoilta/tiedostojen-varmuuskopiointi/
- Hive systems. (2024). Are your passwords in the green? https://www.hivesystems.com/blog/are-your-passwords-in-the-green
- IBM Technology. (2.5.2023). Security Operations Center (SOC) Explained [Video]. YouTube. https://www.youtube.com/watch?v=OHkWXFheSKM&ab_channel=IBMTechnology
- Jyvsectec. (2024). Kyberhäiriöiden hallinta – Käsikirja terveydenhuollon toimijoille. https://jyvsectec.fi/2021/01/kyberhairioiden-hallinta-kasikirja-terveydenhuollon-toimijoille/
- Kyberturvallisuuskomitea (2017). Kodin kyberopas. – ohjeita digitaaliseen arkeen. https://turvallisuuskomitea.fi/viestinta/julkaisut/
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 784/2021. https://www.finlex.fi/fi/laki/alkup/2023/20230703
- Microsoft. (2024). Create and use strong passwords. https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb
- Microsoft. (2024). Auta suojaamaan Outlook.com-sähköpostitilisi. https://support.microsoft.com/fi-fi/office/auta-suojaamaan-outlook-com-s%C3%A4hk%C3%B6postitilisi-ad740fc5-4307-4ece-8231-6d4d4bd8a9ba
- Microsoft. (2024). Mitä on tietojenkalastelu? https://www.microsoft.com/en-security/business/security-101/what-is-phishing
- Microsoft. (2024). VPN-yhteyden muodostaminen Windowsissa. https://support.microsoft.com/fi-fi/windows/vpn-yhteyden-muodostaminen-windowsissa-3d29...b1-f497-f6b7-7633-115722c1...

Lähteet

- Microsoft. (2024). What is ransomware? https://learn.microsoft.com/en-us/security/ransomware/human-operated-ransomware
- Ontrack. (2022). Kuinka vältät kiristysohjelmia tänä päivänä? https://www.ontrack.com/fi-fi/blog/kuinka-vattat-kiristysohjelmia-tana-paivana
- Pirha. (2024). Henkilötietojen tietoturvaloukkaus. https://www.pirha.fi/henkilotietojen-tietoturvaloukkaus
- Sairaanhoitajat. (2021). Digitaaliset taidot osana sairaanhoitajan työtä. https://sairaanhoitajat.fi/ammatti-ja-osaaminen/digitaaliset-taidot-osana-sairaanhoitajan-tyota/
- Siun SOTE. (2024). Toimintaohje: Tietosuoja- ja tietoturvakäsikirja. https://www.siunsote.fi/sosiaali-ja-terveysala?inheritRedirect=true
- STM. (2019). Kyberturvallisuus: Ohje sosiaali- ja terveydenhuollon toimijoille. https://julkaisut.valtioneuvosto.fi/handle/10024/161683
- THL. (2024). Kirjaaminen. https://thl.fi/aiheet/tiedonhallinta-sosiaali-ja-terveysalalla/kirjaaminen
- THL. (2024). Opas sosiaali- ja asiakastietojen käsittelystä täydentää kirjaamisen kokonaisuutta. https://thl.fi/-/opas-sosiaali-ja-asiakastietojen-kasittelysta-taydentaa-kirjaamisen-kokonaisuutta
- Tietosuojavaltuutetun toimisto. (2024). Tietoturvaloukkaukset. https://tietosuoja.fi/tietoturvaloukkaukset
- Traficom. (2024). Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi

Lähteet

- Traficom. (2024). Kybersää. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa?toggle=Kybers%C3%A4%C3%A4tiedotteet%202024
- Traficom. (2020). Pienyritysten kyberturvallisuusopas. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/uusi-oppaamme-auttaa-vahvistamaan-pienyritysten-kyberturvallisuutta
- Traficom. (2020). SolarWinds Orion Platformin takaovi mahdollisti vakoilun ja tietomurtoja. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/solarwinds-orion-platformin-takaovi-mahdollisti-vakoilun-ja-tietomurtoja
- Traficom. (2023). Turvapostiteemaiset kalasteluviestit johtavat sähköpostitilimurtoihin. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/turvapostiteemaiset-kalasteluviestit-johtavat-sahkopostitilimurtoihin
- Traficom. (2024). Tietojenkalastelu- ja huijausviestien kanssa tulee olla yhä tarkempi. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietojenkalastelu-ja-huijausviestien-kanssa-tulee-olla-yha-tarkempi
- Wikipedia. (2024). Tietoturva. https://fi.wikipedia.org/wiki/Tietoturva
- Wikipedia. (2024). Tietue. https://fi.wikipedia.org/wiki/Tietue
- Wikipedia. (2024). WannaCry ransomware attack. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Liite 2. Webropol palautekyselylomake

Kyselylomake – Palautetta kyberturvallisuusluennosta ja opetusmateriaalista

Kiitos, että osallistuit luennolle. Tämä kysely on osa opinnäytetyötäni ja sen tarkoituksena on kerätä palautetta kyberturvallisuusaiheisen opetusmateriaalin ja luennon tehokkuudesta. Vastaa kysymyksiin rehellisesti. Kaikki vastaukset ovat anonyymejä, eikä yksittäisiä vastauksia voida yhdistää vastaajiin.

Arvioi seuraavat väittämät rastittamalla mielestäsi oikea vaihtoehto.

Ymmärrän, että kyselyyn vastaaminen on vapaaehtoista ja haluan osallistua opinnäytetyön tutkimukseen. O Kyllä

1. Opetusmateriaali (PowerPoint-esitys)

1.1 Opetusmateriaalin sisältö oli selkeä ja ymmärrettävä.

O Samaa mieltä

O Jokseenkin samaa mieltä

O Jokseenkin eri mieltä

O Eri mieltä

1.2 Opetusmateriaalissa esitetyt esimerkit olivat hyödyllisiä.

O Samaa mieltä

O Jokseenkin samaa mieltä

O Jokseenkin eri mieltä

O Eri mieltä

1.3 PowerPoint-esityksen visuaalinen ilme tuki oppimista.

O Samaa mieltä

O Jokseenkin samaa mieltä

O Jokseenkin eri mieltä

O Eri mieltä

2. Luento

2.1 Luennolla esitetyt asiat tukivat kyberturvallisuuden ymmärtämistä hoitotyössä.

O Samaa mieltä

O Jokseenkin samaa mieltä

O Jokseenkin eri mieltä

O Eri mieltä

2.2 Luennoitsijan esitystapa oli selkeä ja mukaansatempaava.

O Samaa mieltä

O Jokseenkin samaa mieltä

O Jokseenkin eri mieltä

O Eri mieltä

2.3 Luennon aikana esitetyt kysymykset ja keskustelut olivat hyödyllisiä.

O Samaa mieltä

O Jokseenkin samaa mieltä

O Jokseenkin eri mieltä

O Eri mieltä

3. Osaamisen arviointi ja kehittyminen

3.1 Arvioi omaa kyberturvallisuustietämystäsi ennen luentoa.

O Erittäin hyvä

O Hyvä

O Kohtalainen

O Heikko

3.2 Arvioi omaa kyberturvallisuustietämystäsi luennon jälkeen.

O Erittäin hyvä

O Hyvä

O Kohtalainen

O Heikko

Kiitos palautteesta! Onko sinulla muita kommentteja, ehdotuksia tai palautetta luennosta tai opetusmateriaalista?