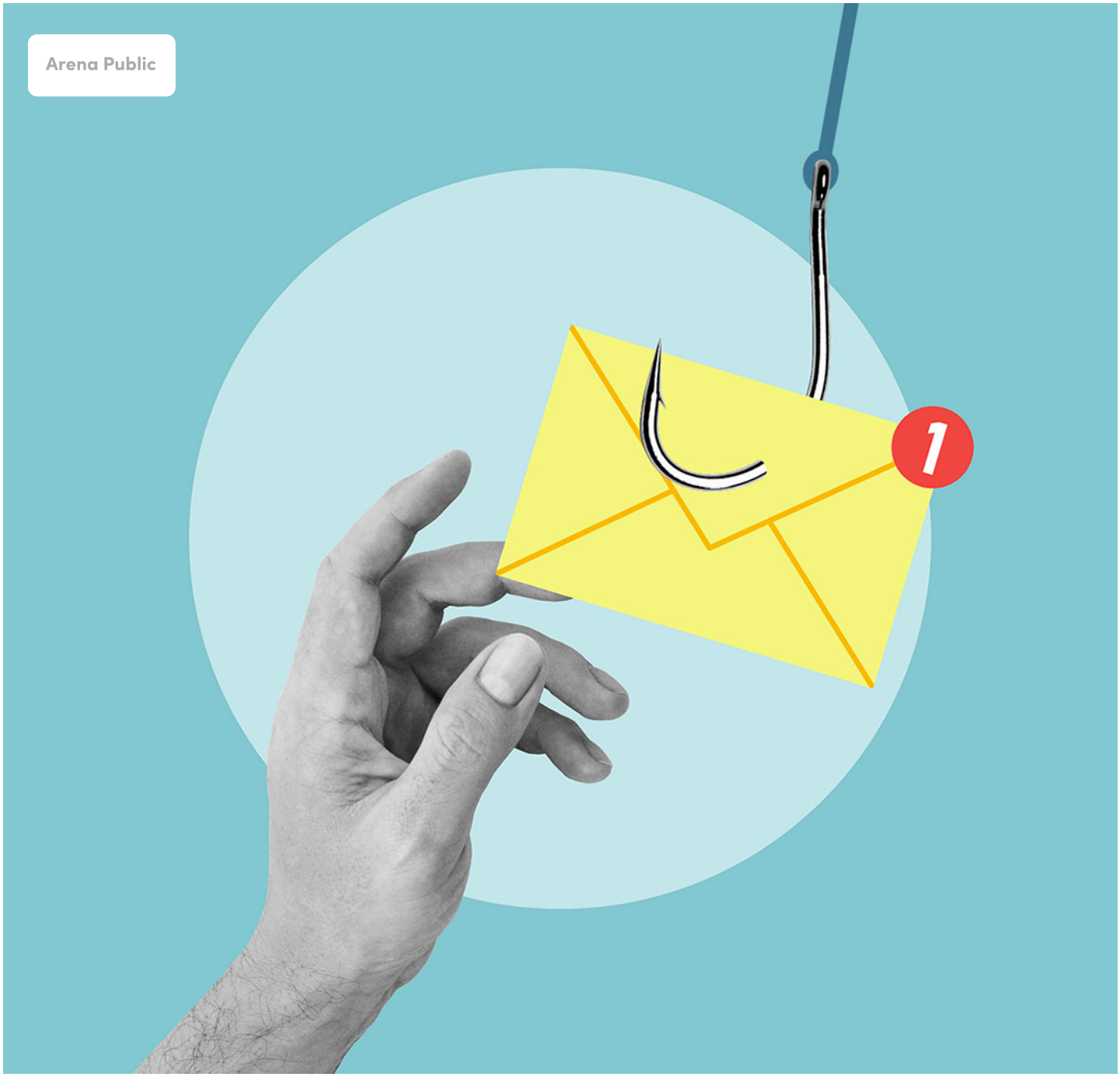

Kuva: Adobe Stock

Miten jokainen oppilaitoksen työntekijä voi vahvistaa kyberturvallisuutta?

valinnoillaan suojatakseen oppilaitoksen digitaalista tietoa ja toimintoja kokonaisvaltaisesti. Mutta mitä tämä tarkoittaa käytännössä ja millaisin keinoin se on toteutettavissa?

5.8.2025
Anna-Liisa Ojala, Tuomo Sipola, Karo Saharinen

Olimme vuoden 2025 alussa Educa-messuilla esittelemässä oppilaitosten kyberturvallisuuteen liittyvää tutkimushankettamme, jota on rahoittanut Työsuojelurahasto. Messuosastollamme kävi paljon aiheesta kiinnostuneita opettajia ja muita oppilaitosten työntekijöitä, ja moni tunnusti tuntevansa aihetta hyvin vähän. Siitä huolimatta usea oppilaitoksen työntekijä kertoi meille, että olemme tärkeällä asialla. Selvästi kyberturvallisuus tunnistetaan jo asiaksi, joka koskee myös oppilaitoksia tavalla tai toisella. Varmasti se myös tunnistetaan asiaksi, josta pitää olla kiinnostunut, vaikka oikeasti toivoisi voivansa pysyä koko aiheesta kaukana. Muutama osallistuja kysyi kuitenkin kysymyksen, joka jäi vaivaamaan myös jälkikäteen: ”Minut on nimetty oppilaitoksemme turvallisuusvastaavaksi, joten miten minun pitää huomioida kyberturvallisuus?” Osa näistä nimetyistä henkilöstä myös kertoi saaneensa nimityksen usein ilman erillistä turvallisuuskoulutusta tai -taustaa.

Mitkä ovat siis ne keskeiset asiat, joihin jokaisen oppilaitoksen työntekijän tulisi perehtyä turvatakseen organisaation kyberturvallisuutta? Tässä artikkelissa tarkastellaankin, mitä asioita turvallisuusvastaavan tai muun henkilöstön jäsenen on syytä huomioida ja edistää kyberturvallisuuden varmistamiseksi oppilaitoksessa. Tarkastelussa hyödynnetään myös Euroopan unionin kyberturvallisuusdirektiivin, NIS2:n (*Network and Information Security Directive 2*) periaatteita organisaatioille kyberturvallisuuden varmistamisessa (Euroopan parlamentin ja neuvoston direktiivi 2022/2555 verkko- ja tietojärjestelmien turvallisuudesta). Tässä tekstissä oletetaan kuitenkin, että oppilaitoksen tietohallinto tai IT-palveluista vastaava taho keskittyy tietojärjestelmien tekniseen valvontaan ja suojaukseen, kuten oppilaitoksen IT-infrastruktuurin säännölliseen tarkistamiseen ja päivittämiseen sekä käyttöoikeuksien hallintaan. Näin ollen keskitymme tässä tavallisten oppilaitostoimijoiden, kuten opettajien, opintosihteerien, rehtorien tai opinto-ohjaajien toimintaan sekä arjen varautumiseen.

Mistä puhumme, kun puhumme kyberturvallisuudesta?

Kyberturvallisuus on laaja käsite, joka liittyy läheisesti myös *tietosuojan* ja *–turvan* käsitteisiin, jotka esitellään tässä tehden synteesiä kansallisista ja kansainvälisistä eri maiden määritelmistä (Suomen kyberturvallisuusstrategia 2024–2035; Maurer & Morgus, 2014). *Tietosuojalla* tarkoitetaan yksilöihin, organisaatioihin ja teknologioihin liittyvien tietojen suojaamista, ja suojaaminen perustuu tyypillisesti oikeudellisiin viitekehyksiin, kuten

turvaamisella pyritään estämään luvaton pääsy, muuttaminen, tuhoaminen tai väärinkäyttö tiedoissa tai tietojärjestelmissä. Kyberturvallisuus on käsitteistä laajin, ja se tarkoittaa suojaavia toimenpiteitä kyberuhkia vastaan, jotka kohdistuvat viestintä- ja tietojärjestelmiin sekä muihin sähköisiin järjestelmiin tai niissä säilytettäviin, käsiteltäviin ja siirrettäviin tietoihin sekä näiden järjestelmien käyttäjiin, hyödyntäjiin ja muihin osapuoliin. Tässä tekstissä kyberturvallisuuden alle lukeutuvat myös tietosuojan ja tietoturvan käsitteet, jollei ole tarve puhua käsitteistä erikseen.

Koska digitaaliset järjestelmät ovat ihmisten suunnittelemia ja käyttämiä sekä toisinaan myös ihmisten toteuttaman haittatoiminnan kohteita, liittyy kyberturvallisuus väistämättä ihmisten toimintaan (Althonayan & Andronache, 2018). Kyberuhat eivät synny vain teknisistä heikkouksista, vaan usein juuri inhimillisistä valinnoista ja virheistä, jotka tehdään joko vahingossa tai tarkoituksella. Siksi ihmisellä on keskeinen rooli sekä uhkien lähteenä että suojan rakentajana (Cains ym., 2021). Tästä syystä kyberturvallisuus ei voi rajoittua pelkästään teknisiin ratkaisuihin, vaan sen on ulotuttava myös käyttäjien toimintaan, asenteisiin ja osaamiseen

Kyberturvallisuuden yhteydessä puhutaan usein *uhkista, riskeistä, digitaalisesta omaisuudesta* ja *poikkeamista* (engl. *threats, risks, assets* ja *incidents*). Kyberturvallisuusuhka on tarpeellinen käsite ymmärtää oppilaitostyössä sitä varten, että voidaan pohtia erilaisia skenaarioita mahdollisista oppilaitoksen kyberturvallisuutta uhkaavista toimijoista tai tapahtumista. Uhkat voidaan jaotella Przymusin ja kumppaneiden (2024) tapaan kolmeen katetoriaan: *verkko–* tai *ohjelmistoympäristöihin liittyviin uhkiin* (vaikkapa ohjelmistopäivitysten laiminlyönti); *tunnuksiin liittyviin uhkiin* (kuten samojen salasanojen käyttäminen monissa järjestelmissä); sekä *käyttäytymiseen liittyviin uhkiin* (kuten sähköpostin kautta saapuneiden linkkien klikkaileminen). Kyberturvallisuusriskistä puhuttaessa taas viitataan sen tilanteen ja todennäköisyyden arviointiin ja luokitteluun tiedon perusteella, että joku uhka oikeasti tapahtuu (Lacey, 2009, s. 87). Poikkeama on tapahtunut silloin, kun uhka on realisoitunut ja vaatii toimenpiteitä. Kyberturvallisuuspoikkeama on siis tapahtuma, joka voi vaarantaa tietojärjestelmän tai sen sisältämän tiedon luottamuksellisuuden, oikeellisuuden tai saatavuuden (NIST, 2025b).

Digitaalinen omaisuus taas tarkoittaa Yhdysvaltojen kansallisen NIST-tietoturvakeskuksen (NIST, 2025a) mukaan sellaista resurssia tai kohdetta, jolla on merkitystä organisaatiolle ja sen sidosryhmille ja jota pyritään siksi suojaamaan organisaation kyberturvallisuudessa. Laadultaan digitaalinen omaisuus on usein aineetonta, kuten tietoa, prosesseja, palveluita tai immateriaalioikeuksia, ja niiden menetys tai häiriö toiminnassa voi aiheuttaa haittaa organisaatiolle tai sen jäsenille. NIST kuitenkin tunnistaa, että joskus omaisuus voi olla myös fyysistä, kuten kehitettyjä laitteistoja.

Mihin keskittää huomiota ja resursseja?

omaisuuksiin (tietoihin ja toimintoihin), jotka ovat oppilaitoksen toiminnan kannalta kriittisimpiä. Jos puhutaan perusopetuksesta, lukiosta ja ammatillisesta opetuksesta, niin näissä oppilaitoksissa luonnollisesti opetetaan, myönnetään opintosuorituksia ja tutkintoja sekä ylläpidetään tukitoimintoja, joiden avulla edellisiä voidaan toteuttaa. Tukitoimintoihin kuuluvat niin opiskeluhuollon toiminnot, opiskelijapalveluiden toiminnot kuin henkilöstöhallinnonkin toiminnot. Lisäksi oppilaitokset saattavat olla mukana kehittämishankkeissa. Ammattikorkeakouluihin ja yliopistoihin mentäessä tutkimuksen sekä kehittämis- ja innovaatiotoiminnan merkitys arjen toiminnoissa kasvaa. Kaikissa näissä voidaan tehdä yhteistyötä työelämätoimijoiden kanssa, mutta ammattioppilaitoksissa ja ammattikorkeakouluissa työelämäyhteistyön rooli on lakisääteisestikin merkittävämpi kuin muissa oppilaitoksissa. Onkin luonnollista olettaa, että oppilaitosten ja jokaisen sen työntekijän tulisi turvata oman roolinsa mukaisesti yllä mainittuihin toimintoihin liittyviä tietoja, prosesseja ja välineistöä.

Lisäksi on hyvä huomata kaksi keskeistä asiaa: ensinnäkin, kyberturvallisuuden pääpaino ei ole vain hyökkäyksen estämisessä, vaan myös kyvyssä palautua ja jatkaa toimintaa, jos kyberturvallisuuspoikkeamia tapahtuu (NIST, 2024). Tämä tarkoittaa sitä, että jos edellä mainittuihin oppilaitokselle keskeisiin tietoihin, prosesseihin tai välineistöihin kohdistuu tieto- tai kyberturvallisuuspoikkeamia, on keskeistä pyrkiä palauttamaan toimintaa takaisin normaaliksi mahdollisimman nopeasti samalla kun minimoidaan poikkeamasta aiheutuvia haittoja. Lisäksi suojaamisessa on huomattava oppilaitoksen lakisääteiset velvoitteet. Eli esimerkiksi oppilaiden ja henkilökunnan henkilötietojen suojaaminen ei ole valinnainen riskiarvioon perustuva toimenpide, vaan pakollinen lakivelvoite, jolle Euroopan parlamentin ja neuvoston asetus (2016/679) tietosuojasta, eli GDPR, asettaa minimitason. Lisäksi on joukko muita oppilaitosten kyberturvallisuuteen liittyviä direktiivejä, kuten EU:n tekoälyasetus (Euroopan parlamentin ja neuvoston asetus 2024/1689), jotka säätelevät oppilaitosten digitaalista arkea eri tavoin.

NIS2-direktiivi oppilaitoksen kyberturvallisuuden tukena

Oppilaitokset ja niiden toiminta ei lukeudu Euroopan unionin Kyberturvallisuusdirektiivin NIS2:n listaamiin erityisen kriittisiin tai muihin kriittisiin toimialoihin yhteiskunnassa (Euroopan parlamentin ja neuvoston direktiivi 2022/2555 verkko- ja tietojärjestelmien turvallisuudesta). Näin ollen NIS2-direktiivi ei määrittele oppilaitosten toimintaa ja infrastruktuuria sellaisiksi kohteiksi, joita olisi erityisesti syytä suojata direktiivin määrittämin toimin. Se ei kuitenkaan tarkoita, etteikö oppilaitosten tulisi varautua ja toimia kyberturvallisuutta vaalien toiminnassaan. Erityisesti NIS2:n huomioiminen on paikallaan niille oppilaitoksille, jotka kouluttavat työvoimaa kriittisille toimialoille tai tekevät yhteistyötä kriittisten toimialojen kanssa, eli ammatillisen koulutuksen oppilaitoksille sekä korkeakouluille. Vaikka NIS2-direktiivi ei suoraan velvoita oppilaitoksia, sen vaatimukset ja suositukset tarjoavat käyttökelpoisen rungon

Direktiivi korostaa erityisesti johdon vastuuta, eli kyberturvallisuus ei voi olla pelkästään IT-henkilöstön harteilla, vaan se vaatii oppilaitoksen johdon sitoutumista kyberturvallisuuteen ja sen johtamiseen. Tämä tarkoittaa esimerkiksi sitä, että oppilaitoksessa laaditaan tietoturvaan liittyviä ohjeita, määritellään vastuut kyberturvallisuuteen liittyen, ja pidetään myös huolta siitä, että resurssit riittävät tarvittaviin toimiin suojauksen ja poikkeamahallinnan osalta. Oppilaitoksella tulee olla suunnitelma sellaisten tilanteiden varalle, joissa tietojärjestelmä ei toimi, tietoa katoaa tai kyberhyökkäys uhkaa keskeyttää opetuksen. On tärkeää tietää, kuka reagoi, miten ja missä aikataulussa, ja miten viranomaisiin ollaan yhteydessä.

NIS2 painottaa myös henkilöstön osaamista, ja henkilöstö tarkoittaa tässä yhteydessä koko oppilaitoksen henkilökuntaa ja myös opiskelijoita. Eli oppilaitoksessa tulee varmistaa, että henkilöstö ja opiskelijat saavat koulutusta arjen tietoturvasta. Koulutuksen aiheet voivat liittyä esimerkiksi seuraaviin teemoihin:

- Miten tunnistetaan huijausviestit?
- Mitä pitää tehdä, jos oppilastietojärjestelmä ei toimi normaalisti?
- Miten salasanat kannattaa luoda ja miten niitä tulisi ylläpitää?
- Saako oppilaitostyössä käyttää omia laitteistoja?
- Mitä pitää tehdä, jos salasana tai opiskelijoiden tai henkilöstön henkilötietoja on päätynyt vääriin käsiin?
- Mitä pitää tehdä, jos opiskelijan vanhempi kyselee opiskelijan tietoja, joiden saamiseen hänellä ei ole oikeutta?
- Miten pitää huolehtia sidosryhmien tieto- ja kyberturvallisuudesta?
- Miten toimitaan tiedonjaon kanssa toimittaessa rajapinnoilla esimerkiksi hyvinvointialueiden kanssa?

Näiden koulutusten teemassa ei pidä keskittyä teknisten ratkaisujen ymmärtämiseen, vaan toiminnan ja ohjeistusten selkeyteen, roolituksiin ja valmiuksiin tunnistaa ja toimia erilaisissa tilanteissa. Säännöllinen perehdytys, käytännönläheiset ohjeet ja selkeä viestintä tukevat arjen toimintaa ja ehkäisevät inhimillisiä virheitä. Kun henkilöstö ja opiskelijat kokevat, että heidän toimintansa on tärkeä osa koulun turvallisuutta, tietoisuus kasvaa luonnollisesti osaksi jokapäiväistä työskentelyä.

Lisäksi on hyvä huomioida, että NIS2 velvoittaa oppilaitoksia välillisesti siinä kohtaa, jos oppilaitoksen opiskelija tai henkilöstö tekee yhteistyötä esimerkiksi kriittisellä toimialalla toimivan yrityksen tai julkisen organisaation kanssa vaikkapa työharjoittelun, opinnäytetyön tai jonkunlaisen tietojärjestelmäintegraation kautta. Tällöin oppilaitoksesta tulee käytännössä NIS2:n määrittämä kolmas osapuoli kyseisen kriittisen toimijan toimitusketjussa. NIS2-direktiivin mukaan kriittisten sektoreiden toimijoilla on velvollisuus varmistaa, että heidän kumppaninsa,

ohjeistettua, ja poikkeamat pystytään tunnistamaan ja raportoimaan. Tämän vuoksi oppilaitoksen kannattaa myös miettiä omaa osuuttaan osana laajempaa turvallisuusverkostoa ja varmistaa, että myös yhteistyöhön liittyvät tekniset ja organisatoriset kyberturvakäytännöt ovat kunnossa.

On myös hyvä huomata, että Suomen kansallinen Kyberturvallisuuskeskus, joka toimii osana Traficomia, on keskeinen kansallinen toimija NIS2-direktiivin täytäntöönpanossa ja valvonnassa. Esimerkiksi kun NIS2:n mukaan merkittävistä tietoturvapoikkeamista on ilmoitettava viranomaiselle 24 tunnin sisällä, niin Suomessa nämä ilmoitukset tehdään Kyberturvallisuuskeskukselle. Vaikka Kyberturvallisuuskeskuksella ei ole velvollisuutta auttaa oppilaitoksia jokaisessa yksittäisessä tapauksessa, on sillä lakisääteinen tehtävä tukea ja ohjeistaa myös kaikkia suomalaisia oppilaitoksia kyberturvallisuudessa. Eli jos vaikkapa kesälomalla ei saisi oppilaitoksen tietoturvavastaavaa kiinni ja epäilisi, että poikkeamaepäilyyn on saatava apua, niin Kyberturvallisuuskeskus tarjoaa tukea puhelimen ja sähköpostin välityksellä.

Yhteinen vastuu arjen turvallisuudesta

Educa-messujen keskustelut vahvistivat sen, mitä olimme jo tutkimushankkeemme aikana havainneet: kyberturvallisuus koskee oppilaitoksia yhä enemmän osana jokapäiväistä työtä ja vuorovaikutusta. Monelle opettajalle, rehtorille tai opintosihteerille kyberturvallisuus voi näyttäytyä epämääräisenä ja teknisenä ilmiönä, joka on helppo ulkoistaa oppilaitoksen IT-osastolle tai palveluntarjoajille. Tämä osoittaa, että tarve ymmärrettävälle ja konkreettiselle tiedolle on ilmeinen.

Kyberturvallisuus ei edellytä, että jokainen koulun työntekijä osaa lukea lokitiedostoja tai arvioida tietoliikenteen salausprotokollia. Sen sijaan oppilaitoksen kyberturvallisuus edellyttää selkeitä toimintatapoja, rohkaisua, koulutusta ja turvallisuustekoja arjen keskellä. Oppilaitoksen henkilöstön ja opiskelijoiden pitää tietää, kenelle voi ilmoittaa poikkeamasta ja pitää saada koulutusta siihen, että osaa tunnistaa epäilyttäviä sähköposteja tai estää vaikutusyritykset vaikkapa opintosuoritusten myöntämisprosesseissa tai henkilötietojen käsittelyssä. Kyberturvallisuus vahvistuu selkeästi ohjeistettujen prosessien ja ennen kaikkea niitä toteuttavien ihmisten kautta; eli juuri niiden koulun arjessa toimivien opettajien, koulunkäyntiavustajien, rehtorien, opintosihteerien, kuraattorien, opiskelijoiden tai vaikkapa siistijöiden kautta, jotka tekevät työpäiviensä aikana satoja valintoja, joiden seuraukset voivat joko lisätä tai heikentää koko organisaation kyberturvallisuutta. Siksi on tärkeää, että kyberturvallisuus ei jää IT-vastaavan tai yksittäisen turvallisuusvastaavan harteille, vaan että se jaetaan kaikkien vastuuksi kullekin roolille sopivalla tavalla.

opiskelijahallintojärjestelmät, sähköiset oppimisalustat, oppilaiden ja opintojen tiedot, suoritustenmyöntöprosessit ja henkilöstön tiedot, mutta muitakin voi omasta oppilaitoksesta löytyä. Mieti suojauksen prioriteettia, eli mikä tieto ja järjestelmä on erityisen herkkää ja mikä vähemmän herkkää ja miksi.

NOSTO 2: Muista, että kyberturvallisuus ei ole vain IT-asiantuntijoiden vastuulla, vaan jokainen oppilaitoksen työntekijä vaikuttaa siihen omilla toimillaan ja valinnoillaan. Pohdi omassa roolissasi, miten voisit toimia esimerkiksi silloin, kun saat outoja sähköposteja, käsittelet opiskelijatietoja vaikkapa hyvinvointialueen työntekijöiden kanssa tai jos sovit ZOOM-kokouksen, jossa käsitellään arkaluontoisia aiheita. Onko sinulla sama salasana monessa järjestelmässä työpaikalla ja sen ulkopuolella? Tiedätkö, keneltä voit kysyä apua valintoihisi tai kenelle voit ilmoittaa epäilyttävästä tilanteesta? Pienet teot arjessa rakentavat koko organisaation tietoturvaa.

NOSTO 3: Jos olet oppilaitoksessasi nimetty turvallisuusvastaavaksi, vaikka ilman erityistä koulutusta, sinun tärkein tehtäväsi ei ole osata kaikkea itse, vaan huolehtia siitä, että tieto ja vastuut ovat selkeitä. Laadi tai pyydä oppilaitoksen johdolta selkeät ohjeet poikkeustilanteiden varalle: kuka tekee mitä, milloin ja kenelle ilmoitetaan? Varmista myös, että työntekijöillä on matala kynnys kysyä ja ilmoittaa epäilyistä. Varmista myös, että henkilöstölle ja opiskelijoille järjestetään koulutusta tasaisin väliajoin.

Avainsanat:

kyberturvallisuus oppilaitokset tietosuoja tietoturva

Kirjoittajat:

Vanhempi asiantuntija

Jyväskylän ammattikorkeakoulu

Toimin TKI-työhön keskittyvänä vanhempana asiantuntijana Jyväskylän ammattikorkeakoulun ammatillisessa opettajakorkeakoulussa (AOKK).

Tuomo Sipola

Vanhempi tutkija

Jyväskylän ammattikorkeakoulu

Olen vanhempi tutkija Jyväskylän ammattikorkeakoulun IT-instituutissa.

Karo Saharinen

Lehtori

Jyväskylän ammattikorkeakoulu

Työskentelen Jyväskylän ammattikorkeakoulun IT-instituutissa lehtorina.

Lähteet:

Althonayan, A. & Andronache, A. (2018). *Shifting from information security towards a cybersecurity paradigm.* ICIME 2018: Information management and engineering. https://doi.org/10.1145/3285957.3285971

Euroopan parlamentin ja neuvoston asetus 2016/679. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32016R0679

Euroopan parlamentin ja neuvoston asetus 2024/1689 tekoälystä (AI Act). https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Euroopan parlamentin ja neuvoston direktiivi 2022/2555 verkko- ja tietojärjestelmien turvallisuudesta. https://eur-lex.europa.eu/legal-content/fi/LSU/?uri=oj:JOL_2022_333_R_0002

Force, J. T. (2018). *Risk management framework for information systems and organizations.* NIST Special Publication 800–37. National Institute of Standards and Technology.

Lacey, D. (2009). *Managing the human factor in information security*. Wiley.

Maurer, T. & Morgus, R. (2014). *Compilation of existing cybersecurity and information security related definitions*. Report. New America.

NIST (2024). *The NIST Cybersecurity Framework 2.0*. National Institute of Standards and Technology. Haettu 25.6.2025 osoitteesta https://doi.org/10.6028/NIST.CSWP.29

NIST (2025a). *Asset*. NIST Computer Security Resource Center Glossary. Haettu 25.6.2025 osoitteesta https://csrc.nist.gov/glossary/term/asset

NIST (2025b). *Incident*. NIST Computer Security Resource Center Glossary. Haettu 25.6.2025 osoitteesta https://csrc.nist.gov/glossary/term/incident

Przymus, Z., Małagocka, K., & Przybyszewski, K. (2024). The human factor in cybersecurity: from risk profiles to resilience. *Procedia Computer Science, 246*, 1437–1445.

Suomen kyberturvallisuusstrategia 2024–2035. Valtioneuvoston kanslian julkaisuja 2024:11. Valtioneuvoston kanslia. http://urn.fi/URN:ISBN:978-952-383-376-0

kyberturvallisuus oppilaitokset tietosuoja tietoturva

Julkaistu
5.8.2025

Arena Public
ISSN 2984-0791

URN
https://urn.fi/urn:nbn:fi:jamk-issn-2984-0791-226

Viittausohje
Ojala, A-L., Sipola, T. & Saharinen, K. (2025). Miten jokainen oppilaitoksen työntekijä voi vahvistaa kyberturvallisuutta? Jamk Arena Public. https://urn.fi/urn:nbn:fi:jamk-issn-2984-0791-226

Aiheeseen liittyvää

Kohti yhdenvertaista ja tasa-arvoista vapaata sivistystyötä opintokeskuksissa ›

Salasanojen hallinta on yhä ajankohtaista oppilaitoksissa ›

Kyberkestävyyssäädöksellä uusien laitteiden tietoturva samalle lähtöviivalle ›

Kyberturvallisempi Eurooppa: NIS2-direktiivin myötä Suomeen uusi kyberturvallisuuslaki ›

Suomalaisten oppilaitosten valmius kohdata kyberkriisejä

Suomalaisten oppilaitosten valmius kohdata kyberkriisejä -hanke tukee oppilaitosten kyvykkyyttä tunnistaa ja kohdata erilaisia kyberturvallisuuteen liittyviä poikkeamia omalla toimialallaan. Tutkimus koskee erityisesti ammatillisia oppilaitoksia, mutta opit sopivat muidenkin oppilaitosten käyttöön. Tutkimushankkeen toteutusaika on 1.1.2024 – 31.8.2025, ja se on Työsuojelurahaston rahoittama.

Lue lisää tästä

Työsuojelurahasto
Arbetarskyddsfonden
The Finnish Work Environment Fund

Takaisin ylös