

10 askelta oppilaitosten parempaan kyberturvallisuuteen



1. Johda ja toimi suunnitelmallisesti

- Oppilaitoksen johdon on sitouduttava kyberturvallisuuteen ja varmistettava riittävät resurssit, selkeät prosessit ja koulutus henkilöstölle.
- Turvaa kriittiset tehtävät niin, ettei vain yksi henkilö ole tietoinen tai vastuussa – tämä vähentää riskejä.
- Huolehdi, että myös ilta-, viikonloppu- ja loma-aikoina on selkeä suunnitelma poikkeamien havaitsemiseen ja hoitamiseen.

2. Suojaa kriittiset tiedot ja järjestelmät

- Tunnista oppilaitoksen ja kunkin työroolin tärkeimmät järjestelmät, ja käytä niitä vain ohjeiden mukaan.
- Tunnista oppilaitoksen ja kunkin työroolin tärkeimmät digitaaliset omaisuudet, ja suojaa niitä.
- Hallinnoi pääkäyttäjyyksiä selkeästi ja turvallisesti. Varmista, että pääkäyttäjät on selkeästi nimetty, heidän käyttöoikeutensa ovat ajantasaiset ja heillä on selkeät ohjeet turvalliseen toimintaan.

3. Tiedosta keskeiset toiminnot ja suojaa niitä

- Tunnista oppilaitoksen ydintehtävät ja prosessit (yleensä opetus sekä suoritusten ja tutkintojen myöntäminen) ja suojaa niitä poikkeamilta ja vaikuttamisyrittäyksiltä.
- Ammatillisissa oppilaitoksissa voi olla myös aitoa asiakasdataa esimerkiksi autokorjaamoissa tai kampaamoissa, jolloin myös näitä oppimiskäytäntöjä tulee suojata erityisellä tarkkuudella.
- Opiskelijat on ohjeistettava huolellisesti harjoitteluissaan, jotta he osaavat suojata myös harjoitteluyrityksen tai -organisaation toimintoja ja tietoja.
- Huomioi myös sidosryhmien kanssa tehtävä työ, kuten hyvinvointialueiden kanssa toimiminen, ja varmista, että tieto- ja kyberturvallisuus toteutuu yhteistyön kaikissa vaiheissa.

4. Käsittele henkilötietoja huolellisesti

- Käsittele henkilötietoja ohjeiden ja säädösten mukaisesti kaikkialla (esim. GDPR).
- Älä luovuta tietoja ulkopuolisille ilman oikeutettua syytä. Varmista ennen kuin toimit.

5. Käytä vahvoja ja eri salasanoja

- Käytä eri salasanaa jokaiseen järjestelmään, vähintään 12 merkkiä – mieluiten 16.
- Hyödynnä salasananhallintaohjelmaa.
- Ota käyttöön monivaiheinen tunnistautuminen (MFA) aina kun mahdollista – mutta muista, että se ei korvaa vahvan salasanan tarvetta.

6. Käytä omia laitteita ja sovelluksia harkiten

- Noudata oppilaitoksen ohjeita, jos käytät omia laitteita tai sovelluksia työasioihin.
- Varmista, että laite on suojattu ajantasaisilla päivityksillä ja salasanoidella.

7. Pidä taitosi ajan tasalla

- Osallistu tietoturvakoulutuksiin ja seuraa oppilaitoksen ohjeita.
- Kysy IT-tuesta neuvoa, jos olet epävarma.

8. Kiinnitä erityishuomiota kriittisiin toimialoihin

- Oppilaitos voi olla NIS2-direktiivin tarkoittama kolmas osapuoli kriittisen toimialan toimitusketjussa esimerkiksi työelämäyhteistyön, harjoittelun tai opinnäytetöiden kautta – tällöin on pystyttävä osoittamaan turvalliset käytännöt.

9. Tunnista keskeisimmät uhat, kuten huijausviestit

- Älä klikkaa epäilyttäviä linkkejä tai avaa tuntemattomia liitteitä.
- Älä jaa tunnuksia tai salasanoja muille.
- Älä käytä työlaitteita ja työ sähköpostia työtehtävien ulkopuolella.
- Vältä kiirettä toimiessasi askareissa, joissa on tieto- tai kyberturvallisuusriski.
- Jos epäroit, kysy neuvoa IT-tuesta.

10. Varaudu poikkeamiin

- Harjoittele etukäteen, miten toimitaan kyberturvallisuuspoikkeamassa.
- Nopea reagointi, selkeät ilmoituskanavat ja roolit voivat estää vahinkojen laajenemisen.
- Tarvittaessa Traficomin Kyberturvallisuuskeskus tukee ja ohjaa eteenpäin poikkeamahavainnoissa ja niiden selvittelyssä.