



Oamk Journal

Oulun ammattikorkeakoulun julkaisuja

Tämä on alkuperäisen julkaisun rinnakkaistallenne. Rinnakkaistallenne saattaa erota alkuperäisestä sivutuksestaan ja painoasultaan.

This is an electronic reprint of the original publication. This version may differ from the original in pagination and typographic detail.

Käytä viittauksessa alkuperäistä lähdettä/Please cite the original version:

Koho, S. (2024). Turvallisesti ja vastuullisesti. Teoksessa Satu Koho (toim.), *Vahvaa viestiä digisti: Opas kiinnostavaan, tavoittavaan ja turvalliseen digitaaliseen viestintään* (s. 9-13). Oulun ammattikorkeakoulu. <http://urn.fi/urn:isbn:978-951-597-251-4>

Oikeudet: CC BY-SA 4.0

2 Turvallisesti ja vastuullisesti

Satu Koho

Journalismin yliopettaja ja

Vahva viesti -hankkeen projektipäällikkö



2.1 Suojaa, tunnista ja torju

Digitaalinen turvallisuus on luotettavan faktapohjaisen tiedon elinehto, aina tiedon hankinnasta sen säilyttämiseen ja jakamiseen.

Journalistien ja muiden viestijöiden on pystyttävä suojaamaan itsensä, lähteensä ja työnsä. Tämä edellyttää digitaalista itsepuolustusta – ennen kaikkea keinoja ja välineitä, joilla tunnistaa ja torjua kyberuhkia ja disinformaatiota.

Seuraavissa alaluvuissa tarkastellaan, mitä digiympäristössä toimivan viestijän tulisi huomioida ja miksi. Lisäksi esitellään digiturvaan liittyviä työkaluja ja toimintatapoja.

2.2 Käsitteet auki

Tietoturva tarkoittaa sitä, että tietoja ja kokonaisia IT-ympäristöjä suojataan niin, etteivät ne joudu väärin käsiin eivätkä katoa tai muutu. Tietyillä toimenpiteillä, kuten asettamalla vahvat salasanat ja palomuurit sekä huolehtimalla varmuuskopioinnista ja varayhteyksistä, pyritään varmistamaan, että tietoja käsitellään oikein ja turvallisesti.

Tietosuoja tarkoittaa yksityisyyden ja henkilötietojen kunnioittamista ja suojaamista. Kyseessä on perusoikeus, joka on kirjattu EU-alueen yleiseen tietosuoja-asetukseen eli [GDPR-lakiin](#). Laki sääntelee henkilötietojen keräämistä, käsittelyä ja luovuttamista sekä niihin liittyviä oikeuksia ja velvollisuuksia. Kansallinen [Tietosuojalaki](#) täsmentää ja täydentää GDPR-lakia.

Disinformaatio on tahallisesti levitettyä väärää tai harhaanjohtavaa tietoa, jonka tarkoituksena on vaikuttaa mielipiteisiin ja/tai käyttäytymiseen. Asioita vääristellään ja niistä valehdellaan, kuva- ja äänimateriaalia manipuloidaan, salaliittoteorioita levitetään. Disinformaation tarkoituksena on aiheuttaa hämmennystä, epäluuloa, pelkoa ja jopa vihaa. Pahimmillaan se näivertää demokratiaa, polkee ihmisoikeuksia ja aiheuttaa sekasortoa. Disinformaatio on merkittävä turvallisuushuhtaus.

Kyberympäristö on alati muuttuva ja monimutkainen digitaalinen ympäristö, jossa digitaalista tietoa vastaanottavat ja lähettävät laitteet ovat yhteydessä toisiinsa erilaisten verkkojen (esimerkiksi mobiili- ja satelliittiverkot ja internet) sekä palveluiden, kuten sähköpostin, pilvipalveluiden ja sosiaalisen median, kautta.

Kun joku – esimerkiksi luotettavana esiintyvä hyökkääjä, vakoilija, kilpailija tai vieras valtio – yrittää vahingoittaa, varastaa tai muuttaa kyberympäristössä olevia tietoja tai järjestelmiä, puhutaan kyberuhkasta. Uhka voi kohdistua niin yksityishenkilöihin kuin vaikkapa toimittajiin ja mediayrityksiin, viranomaisiin ja koko yhteiskuntaan. Erityisesti journalisteihin kohdistuvia kyberuhkia ovat tietojen verkkourkinta (phishing), syväväärennös (deepfake) ja palvelunestohyökkäys (DDoS).

Haittaohjelmat keräävät, varastavat, muuttavat tai tuhoavat tietoja. Ne leviävät muun muassa sähköpostin, verkkosivujen, tiedostojen tai tietokoneeseen liitettävien laitteiden ja kaapeleiden kautta. Haittaohjelmat voivat olla esimerkiksi laitteen tuhoavia viruksia, roskaposti-, vakoilu- ja kiristysohjelmia tai troijalaisia levittäviä valepäivityksiä.

2.3 Organisaatio pääsee vähemmällä

Mediayhtiöistä koostuvan [Mediapoolin](#) tehtävänä on kehittää media-alan varautumista kriisi- ja erityistilanteisiin eli turvata se, että kansalaiset saavat luotettavaa tietoa kaikissa olosuhteissa.

Mediapooli on tuottanut kattavan [kybersuosituspaketin](#), joka sisältää ohjeita varautumiseen mutta myös tilanteisiin, joissa riski on jo toteutunut.

Ohjeissa korostetaan, että vaikka kyberriskeistä tiedetään ja ne on minimoitu, hyökkääjä voi päästä organisaation käyttämiin järjestelmiin. Ratkaisevaa on, että hyökkäys havaitaan nopeasti ja osataan toimia. Niinpä organisaatiossa tulisi olla valmiit suunnitelmat erilaisten häiriötilanteiden varalle: kuinka vastuut jaetaan, mitä konkreettista tehdään, millaista yhteistyötä tarvitaan muiden yritysten ja viranomaisten kanssa ja miten tilanteesta viestitään niin organisaation sisällä kuin ulospäin yleisölle, asiakkaille ja sidosryhmille. Suunnitelmat päivittyvät ja paranevat harjoittelemalla.

Kyberturvallisuudesta huolehtiminen lähtee organisaatiossa perusasioista:

Käyttöoikeuksia annetaan vain niitä tarvitseville ja monivaiheista tunnistautumista käytetään laajasti. Kriittisten järjestelmien varmuuskopiot turvataan tuhoamiselta. Koodit ja pilvialustat pidetään hallinnassa ja tietoliikenneyhteydet toimivina. Tätä varten selvitetään, onko kaistaleveyttä riittävästi ja varajärjestelmä riippumaton pääjärjestelmästä. Ovatko vaihtoehtoiset reitit tiedossa? Viestintäalalla ei toimita ilman yhteyksiä.

2.4 Digiturvavinkkejä kaikille

Mediapooli ja [Kyberturvallisuuskeskus](#) ovat koonneet sivustoilleen ja oppaisiinsa ohjeita, joita kenen tahansa digiturvastaan huolehtivan kannattaa hyödyntää. Tässä muutama:

- Tunnistaudu monivaiheisesti, myös somessa.
- Käytä eri palveluissa eri salasanoja ja varmista, ettei kukaan saa niitä haltuunsa. Harkitse lisäksi eri käyttäjätunnuksia ja suojaa myös kotireititin vahvalla salasanalla.
- Salasanojen pitäisi olla vahvoja. Vahvuuteen vaikuttavat pituus (yli 14 merkkiä), yllättävyys (lause, joka on helppo muistaa mutta vaikea arvata) ja ainutkertaisuus (joka palvelulle oma vahva salasana).
- Salasanan hallintasovelluksilla (esimerkiksi 1Password, Bitwarden, Enpass ja Keeper) luot ja säilytät salasanaja vaivattomasti.
- Anna puhelinsovelluksille vain välttämättömät oikeudet ja suojaa tärkeät sovellukset pin-koodilla.
- Pidä laitteidesi ja käyttämiesi sovellusten päivitykset ajan tasalla.
- Hoida työasiat työkoneella ja yksityisasiat kotikoneella.
- Älä kytke tietokoneesi tai älylaitteesi usb-porttiin mitään varmistamatonta.
- Vältä julkisia langattomia verkkoja, käytä VPN-yhteyttä.
- Älä haksahda valesivustoihin. Tarkista verkkosivun osoite.
- Mieti, mitä jaat ja kenelle.

2.5 Täsmäohjeita journalisteille



Lähdesuoja on lehdistönvapauden ja tiedonsaannin perusta, mutta se uhkaa rapautua digimaailmassa. Miten tärkeitä tietoja antavaan henkilöön pidetään yhteyttä vaarantamatta hänen turvallisuuttaan? Kuinka viestit salataan ulkopuolisilta? Miten olla lähdekriittinen?



Journalisteihin kohdistuu vakoilua, vaikuttamisyrityksiä ja vihapuhetta, ja siksi kybersuositusten erityisen huolellinen noudattaminen on tärkeää. Uhkailusta, maalittamisesta, lahjontayrityksestä ja identiteettivarkaudesta pitää ilmoittaa työnantajan lisäksi poliisille.



Omia digiturvaitoja on päivitettävä ja testattava – turvallisesti. Mediapoolin sivustolta voi muun muassa ladata maksutta **Toimittajan salausoppaan** ja käydä suorittamassa oppaaseen pohjautuvan **Toimittajan digiturva -verkkokurssin**.

Näin media-alalla työskenteleviä ohjeistetaan toimimaan digimaailmassa:

- Noudata mediatalon kybersuosituksia erityisen huolellisesti.
- Ole kriittinen. Opettele tunnistamaan disinformaatio. Käytä tarvittaessa kuvantunnistusohjelmia, kuten käänteistä kuvahakua (esimerkiksi **Googlen kuvahaku** ja **TinEye**) ja faktantarkistuspalveluita (esimerkiksi **Faktabaari**).
- Sisäistä, mitä laki sanoo tietosuojasta. Käytä tiedon salausta laajasti, jotta erityistä suojaa vaativa ei erotu muusta tiedosta.
- Hyödynnä **Signal-sovellusta** ja salattua sähköpostia. Tärkeän viestiliikenteen voi suojata salausavaimilla. Viestien päästä päähän-salauksessa vain viestin lähettäjä ja vastaanottaja voivat lukea viestin.
- Jätä mahdollisimman vähän jälkiä käynneistäsi eri sivustoilla ja palvelimilla. Käytä monivaiheista tunnistautumista ja salaa selaintiedot.
- Salaa henkilötietosi, jos vain voit. Seuraa, miten nimeäsi käytetään verkossa.

Mediapoolin sivuilla on monia muitakin täsmäohjeita liittyen esimerkiksi digiturvallisuuteen ja matkustamiseen, asiattomiin viesteihin toimittajan tai median sometilillä, identiteettivarkauteen ja tietomurtoon.

Mediapooli

- Osa Huoltovarmuuskeskuksen laajempaa **huoltovarmuusorganisaatiota**, jonka tavoitteena on turvata huoltovarmuuden kannalta kriittisten organisaatioiden ja sitä kautta koko yhteiskunnan toimintaedellytykset kaikissa oloissa.
- Tehtävänä varmistaa, että tiedonvälitys toimii aina, myös kriisi- ja poikkeustilanteissa.
- Mukana mediatoimialan yrityksiä ja niitä tukevia viranomaisia. Toimii hallinnollisesti Medialiiton yhteydessä.
- Verkkosoite: **www.mediapooli.fi**



Lähteet ja lisätietoa

[Freedom House -kansalaisjärjestön maakohtaiset vuosiraportit digitaalisesta turvallisuudesta.](#) Hakupäivä 17.11.2023.

[Joukkoistamista hyödyntävä faktantarkistus.](#) Hakupäivä 17.11.2023.

Jyrkiäinen, Senni & Koskinen, Tero 2023. Työpaja 24.1.2023 ja sen luentomateriaalit.
Vahva viesti -hanke. Oulun ammattikorkeakoulu.

[Kansainvälisen RSF-toimittajajärjestön \(Reporters sans frontières\) turvallisuusohjeita.](#)
Hakupäivä 17.11.2023.

[Kyberturvallisuudesta.](#) Hakupäivä 17.11.2023.

[Käänteiseen kuvanhakuun Google.](#) Hakupäivä 17.11.2023.

[Käänteiseen kuvanhakuun TinEye.](#) Hakupäivä 17.11.2023.

[Muita Mediapoolin julkaisuja ja tallenteita.](#) Hakupäivä 17.11.2023.

[Ohjeita matkustusturvallisuuteen.](#) Hakupäivä 17.11.2023.

[Salasanan tarkistus \(onko hakkeroitu\).](#) Hakupäivä 17.11.2023.

[Tietosuojasta ja GDPR:stä.](#) Hakupäivä 17.11.2023.

[Toimittajan salausopas, jossa muun muassa salaukseen opastetaan vaihe vaiheelta.](#)
Hakupäivä 17.11.2023.

[Toimittajien oikeuksia ja vapauksia puolustavan kansainvälisen CPJ:n \(Committee to Protect Journalists\) sivusto.](#) Hakupäivä 17.11.2023.

[Vuorovaikutteinen turvallisuusopas.](#) Hakupäivä 17.11.2023.

[Yksityisyyden suojaan painottuva Signal-pikaviestisovellus.](#) Hakupäivä 17.11.2023.