Digitaalisen väkivallan kartoituslomake

Lomakkeen tarkoitus

Tällä työvälineellä kartoitetaan aikuisasiakkaiden kokemaa digitaalista väkivaltaa sekä autetaan digitaaliseen väkivaltaan puuttumisessa. Työväline on kehitetty turvakotien käyttöön, mutta sitä voivat hyödyntää muutkin ammattilaiset.

Mitä digitaalinen väkivalta on?

Digitaalisella väkivallalla tarkoitetaan tekoja, joissa toista ihmistä loukataan, kontrolloidaan, tarkkaillaan tai vahingoitetaan tieto- ja viestintäteknologian välityksellä. Teoissa hyödynnetään digitaalista teknologiaa, esimerkiksi pääte-, äly-, paikannus- ja muita vastaavia laitteita, ohjelmistoratkaisuja, sovelluksia ja pikaviestipalveluja. Digitaalinen väkivalta voi olla myös epäsuoraa, jolloin tekijä hyödyntää teoissaan esimerkiksi toisia henkilöitä, kuten yhteisiä lapsia.

Lähisuhteissa digitaalista väkivaltaa tapahtuu usein yhdessä muiden väkivallan muotojen kanssa. Digitaalisen väkivallan muodot voivat olla vaikeasti tunnistettavia, eikä kokija välttämättä tiedosta itse kokevansa digitaalista väkivaltaa.

Digitaalista väkivaltaa on esimerkiksi:

- puhelimessa, verkossa ja sosiaalisen median alustoilla tapahtuva väkivalta, uhkailu ja vainoaminen
- sosiaalisen median ja pikaviestipalvelujen käytön sekä niissä tapahtuvan vuorovaikutuksen kontrollointi
- intiimin tai muun arkaluontoisen yksityiselämään liittyvän tiedon tai kuvamateriaalin levittäminen, sillä uhkailu tai kiristäminen
- henkilökohtaisten sovellusten, tilien, salasanojen ja pankkitunnusten luvaton hallussapito ja käyttäminen
- ei toivottu, jatkuva soittelu tai viestittäminen
- jatkuvasti tavoitettavissa olemisen vaatiminen
- paikannus- ja tallennuslaitteiden sekä -ohjelmien avulla tapahtuva uhkailu, häirintä, vainoaminen ja kontrollointi
- paikantimen asentaminen ja sijainnin seuraaminen sen avulla ilman lupaa.

Kaikilta aikuisasiakkailta kysyttävät ydinkysymykset

Työvälineen alussa on neljä ydinkysymystä, joilla kartoitetaan digitaalisen väkivallan ilmenemistä. Ne on tärkeä kysyä kaikilta aikuisasiakkailta.

Jos asiakas vastaa kaikkiin ydinkysymyksiin ”ei” tai ”ei tietoa”, varmista silti, onko digitaaliseen turvallisuuteen liittyen muita asioita, jotka olisi hyvä huomioida. Tällaisia asioita voivat olla esimerkiksi älylaitteen sijaintitietojen ottaminen pois päältä ja huomion kiinnittäminen some-päivitysten sisältöihin.

Ennen ydinkysymyksiä

Ennen ydinkysymysten esittämistä käy asiakkaan kanssa läpi lomakkeen tarkoitus sekä digitaalisen väkivallan määritelmä ja esimerkit sen ilmenemismuodoista.

Tarpeen mukaan esitettäviä täsmentäviä kysymyksiä

Täsmentäviä kysymyksiä voidaan tarvittaessa esittää asiakkaalle, jos ydinkysymyksillä ei pystytä kartoittamaan tilannetta riittävän tarkasti. Täsmentävillä kysymyksillä ammattilainen voi varmistaa, että asiakas on ymmärtänyt ydinkysymykset oikein. Niiden avulla ammattilainen voi myös esittää tarkennuksia ydinkysymyksen teemaan liittyen.

Mahdollisia toimia ja huomioita digitaalisen väkivallan tilanteissa

Työvälineen lopussa esitetään toimenpide-ehdotuksia tilanteisiin, joissa asiakkaaseen tai hänen läheiseensä, kuten lapseen, kohdistuu tai mahdollisesti kohdistuu digitaalista väkivaltaa. Asiakkaan vastaukset ja toimenpide-ehdotukset huomioidaan, kun hänen kanssaan laaditaan esimerkiksi turvasuunnitelmaa.

Asiakastyön kannalta olennaiset tiedot kirjataan asiakastietojärjestelmään.

Ydinkysymykset	**Valitse sopiva vaihtoehto**	**Työntekijän muistiinpanoja**
1. Koetko tai pelkäätkö, että väkivallan tekijä käyttää digitaalista väkivaltaa sinun tai läheisesi (esim. lapsesi) kontrolloimiseksi tai vahingoittamiseksi?	☐ Kyllä/ mahdollisesti ☐ Ei ☐ Ei tietoa	
2. Onko väkivallan tekijä lähettänyt, tehnyt tai soittanut sinulle tai läheisellesi (esim. lapsellesi) uhkaavia tai väkivaltaisia viestejä, some-päivityksiä tai puheluja?	☐ Kyllä/ mahdollisesti ☐ Ei ☐ Ei tietoa	
3. Tiedätkö tai uskotko, että väkivallan tekijällä on pääsy sinun tai läheisesi (esim. lapsesi) digitaalisiin laitteisiin, käyttäjätileihin tai tiedostoihisi tahtomattasi? (esim. puhelin, tabletti, tietokone, sähköposti, Facebook, WhatsApp, verkkopankkitunnukset, Find my phone, kuvatiedostot, Apple ID)	☐ Kyllä/ mahdollisesti ☐ Ei ☐ Ei tietoa	
4. Tiedätkö tai uskotko, että väkivallan tekijä seuraa sinun tai läheisesi (esim. lapsesi) sijaintia, liikkumista, yhteydenpitoa tai tekemisiä teknologian avulla? (esimerkiksi älylaitteiden, vakoiluohjelmien, paikannuslaitteiden tai sijaintitietojen avulla)	☐ Kyllä/ mahdollisesti ☐ Ei ☐ Ei tietoa	

Täsmentäviä kysymyksiä digitaaliseen väkivaltaan liittyen

Ydinkysymys 1: Asiakkaan tilanne ja huolet	Työntekijän muistiinpanoja
Onko tapahtunut jotakin, mikä herättää sinussa erityistä huolta, ja mitkä asiat huolestuttavat sinua tällä hetkellä eniten?	
Mitä digitaalisia laitteita, sovelluksia ja/tai tilejä sinulla (ja läheisilläsi, kuten lapsillasi) on tällä hetkellä käytössä?	
Käytätkö sinä tai lapsesi tällä hetkellä väkivallan tekijältä saatuja tai yhteiskäytössä olleita laitteita?	
Pelkäätkö, että jonkun toisen (esim. lapsesi, muu sukulainen tai läheinen) teknologian käyttö vaarantaa turvallisuutesi?	
Onko väkivallan tekijällä työn tai kiinnostuksen puolesta erityistä teknistä osaamista?	
Onko väkivallan tekijällä pääsy sinun arkaluontoisiin kuviin, videoihin tai tiedostoihin (esim. päiväkirjat, intiimit kuvat, terveystiedot tms.)?	
Ydinkysymys 3: Väkivallan tekijän pääsy asiakkaan laitteisiin ja tileihin	**Työntekijän muistiinpanoja**
Epäiletkö tai tiedätkö väkivallan tekijän saaneen selville sinun tai lapsesi käyttäjätunnuksen ja salasanan esimerkiksi sähköpostiin, johonkin laitteelle tai sosiaalisen median tilille (esim. Facebook, Instagram, Snapchat)?	
Onko väkivallantekijä asentanut sinun tai lapsesi käytössä oleville laitteille ohjelmistoja tai luonut käytössänne olevia käyttäjätilejä?	
Onko sinun tai lapsesi digitaalinen laite tai käyttäjätili liitetty sovellukseen (esim. Google Family Link), johon myös väkivallantekijällä on pääsy?	

Tietääkö väkivallan tekijä kenen kanssa olet viestitellyt tai vihjaileeko tekijä tietävänsä asioita, joista hänen ei pitäisi olla tietoinen?	
Onko sosiaalisen median tilillesi tullut päivityksiä, jotka eivät ole sinun tekemiäsi?	
Näyttävätkö viestisi luetuilta tai onko niitä poistettu (esim. sähköpostiviestit, Messenger-viestit, WhatsApp-viestit)?	
Oletko löytänyt laitteesi tai tiliesi hakuhistoriasta (esim. Google, Facebook) sinulle tuntematonta hakuhistoriaa?	
Onko tiedostojasi tahtomattasi poistettu esimerkiksi tietokoneelta, puhelimesta tai pilvipalvelusta?	
Onko puhelimestasi tai muusta laitteestasi tai sovelluksestasi poistettu tärkeitä yhteystietojasi?	
Onko sinun nimissäsi tilattu tavaroita, otettu pikavippejä tai tehty sopimuksia?	
Onko sinulle tullut sähköpostiisi tai tekstiviestitse tieto epäilyttävistä kirjautumistapahtumista?	
Onko pankkitililläsi ollut tapahtumia, joita et ole itse tehnyt?	
Onko sinulla ollut ongelmia saada puhelimella tai muulla laitteella yhteyttä haluamiisi tahoihin tai onko muilla ollut ongelmia saada sinuun yhteyttä (puhelinnumero, käyttäjätili tai sähköpostiosoite estetty)?	

Ovatko laitteesi, sähköpostisi tai sosiaalisen median tilisi olleet tai ovatko ne edelleen väkivallan tekijän hallussa?	
Onko sinulla tai lapsellasi käytössä älylaitteita, joiden etäkäyttötunnukset ovat tekijän tiedossa?	
Ydinkysymys 4: Asiakkaan seuraaminen teknologian avulla	**Työntekijän muistiinpanoja**
Seuraako tekijä sinun tai läheisesi (esim. lapsesi) sijaintia tai liikkumista?	
Tietääkö tekijä sinun olinpaikkasi (menneen, nykyisen tai tulevan) vaikka ei pitäisi?	
Onko laitteessasi, autossasi tai mobiilisovelluksessa laitettu sijainnin jakaminen päälle?	
Onko käytössäsi älylaitteita, joita et ole itse asentanut (esimerkiksi navigaattori, eläinten tutkapannat, älykodinkoneet, turvakamerat)?	
Onko sinun tietojasi yritetty hankkia muiden henkilöiden kautta digitaalisin välinein?	

Mahdollisia toimia ja huomioita digitaalisen väkivallan tilanteissa

Varmista aina ensisijaisesti asiakkaan turvallisuus. Arvioikaa tilanne ja toimenpiteet huolellisesti yhdessä asiakkaan ja tarvittavien muiden tahojen kanssa. Joissakin tilanteissa digitaalisen väkivallan vähentämisen toimenpiteet, jotka tulevat väkivallan tekijän tietoon, saattavat lisätä vakavan fyysisen väkivallan riskiä. Tehtävien toimenpiteiden tulee olla suhteessa digitaalisen väkivallan riskiin sekä asiakkaan ja ammattilaisen arvioon.

Jos on syytä epäillä, että asiakkaan laitteessa on vakoilu- tai haittaohjelma, arkaluontoiset yhteydenotot kannattaa tehdä turvallisella laitteella.

Harkittavia toimia jos asiakkaaseen kohdistuu tai mahdollisesti kohdistuu digitaalista väkivaltaa:

- Vakavan parisuhdeväkivallan riskiarvio (MARAK)
- Häirinnän ja vainon riskinarvio
- Poliisin konsultaatio / ilmoitus poliisille
  - Jos epäillään vakoilulaitetta tai -ohjelmaa, ollaan ensisijaisesti yhteydessä poliisiin. Mikäli asiakas ei halua olla poliisiin yhteydessä, myös esimerkiksi yksityisillä yrityksillä ja järjestöillä on tarjolla digitaaliseen turvallisuuteen liittyvää osaamista.
- Kuvakaappaukset uhkaavista viesteistä/epäilyttävistä ohjelmista
  - Kuvakaappaukset voivat toimia todistusaineistona. Kuvakaappaukset on perustelua ottaa välittömästi sillä tekijä voi poistaa viestit tai ohjelmat.
- Salasanojen vaihtaminen
  - Salasanan voi vaihtaa esimerkiksi turvakodin tietokoneella, jos salasanan vaihtaminen ei ole turvallista asiakkaan omalla laitteella. Ohjeista asiakasta turvallisen salasanan luomisessa, jota väkivallan tekijä ei voi esimerkiksi arvata.
- Liittymien ja digitaalisten tilien vaihtaminen
  - Kartoittakaa tarvittaessa asiakkaalla olevat liittymät ja tilit sekä arvioikaa onko tarvetta irtisanoa tai vaihtaa liittymiä tai tilejä tai luoda uusia tilejä (esimerkiksi luoda uusi sähköpostiosoite asiakkaalle).
- Tehdasasetusten palauttaminen
  - Toimenpide hävittää todistusaineiston, kuten mahdollisesti asennetun vakoiluohjelman sekä muut asiakkaalle tärkeät tiedostot kuten valokuvat. Varmista, että todistusaineisto ja asiakkaalle tärkeät tiedostot on otettu talteen ennen toimenpidettä. Ota tarvittaessa kuvakaappaus haittaohjelmasta ja muista mahdollisista todisteista.
- Laitteen lentokonetilaan laittaminen
  - Laite voidaan kytkeä lentokonetilaan esimerkiksi siihen saakka, kunnes laite on toimitettu poliisille (mikäli laitteeseen on asennettu esim. vakoiluohjelma).
- Sammuta bluetooth-laitteet ja puhelimen bluetooth-yhteys
  - Esimerkiksi älykellot, älysormukset ja langattomat kuulokkeet voivat siirtää tietoa käyttäjän sijainnista.
- Tarkista laitteet viruksentorjuntaohjelmalla
  - Tarjolla on maksullisia ja maksuttomia ohjelmia.
- Älylaitteiden vaihtaminen
  - Laitteen vaihtamisen yhteydessä voidaan luoda myös uudet tilit, joihin väkivallan tekijällä ei ole pääsyä (esim. google-tili, icloud-tili)
- Verkkopankkitunnusten vaihtaminen, maksukorttien kuoletus, oman pankkitilin avaaminen
- Muiden korttien vaihtaminen tai kuoletus, joista esim. asiakkaan osoitetiedot on saatavissa tai tekijä voi aiheuttaa vahinkoa (esim. bonuskortit, kirjastokortit, museokortti jne.)
  - Kartoittakaa tarvittaessa asiakkaalla olevat kortit ja arvioikaa onko tarvetta vaihtaa tai kuolettaa kortteja.
- Kaksivaiheisen tunnistautumisen käyttöönotto