3.8.2021

Digitaalisen väkivallan tunnistaminen ja siihen puuttuminen turvakodeissa

Tällä työvälineellä kartoitetaan turvakotien aikuisasiakkaiden kokemaa digitaalista väkivaltaa sekä autetaan digitaaliseen väkivaltaan puuttumisessa. Digitaalisella väkivallalla viitataan tekoihin, joilla toista ihmistä pyritään vahingoittamaan tai kontrolloimaan teknologiaa hyväksikäyttäen.

Työvälineen käyttö turvakodissa

Työväline on tarkoitettu työntekijän käytettäväksi yhdessä aikuisasiakkaan kanssa, osana hänen kokonaistilanteen kartoitusta. Työvälinettä on perusteltua käyttää turvakotijakson alkuvaiheessa, jotta mahdollisesti edelleen turvakodissa jatkuva digitaalinen väkivalta voidaan tunnistaa ja asiakasta voidaan auttaa.

Kaikilta aikuisasiakkailta kysyttävät ydinkysymykset

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

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

Tarpeen mukaan esitettäviä täsmentäviä kysymyksiä

Täsmentäviä kysymyksiä voidaan tarvittaessa esittää asiakkaalle, jos ydinkysymyksillä ei pystytä kartoittamaan tilannetta riittävän tarkasti. Ammattilainen voi varmistaa täsmentävillä kysymyksillä, että asiakas on ymmärtänyt ydinkysymykset oikein tai esittää tarkennuksia ydinkysymyksen teemaan liittyen.

Huomiot ja toimenpide-ehdotukset

Työvälineen lopussa on huomioita ja toimenpide-ehdotuksia, jos asiakkaaseen kohdistuu tai mahdollisesti kohdistuu digitaalista väkivaltaa.

Asiakastyön kannalta olennaiset tiedot kirjataan asiakastietojärjestelmään.

Digitaalisen väkivallan kartoitus

Ydinkysymykset	Ympyröi sopiva vaihtoehto	Työntekijän muistiinpanoja
1. Oletko huolissasi, että väkivallan tekijä käyttää digitaalisia laitteita tai sovelluksia sinun tai läheisesi (esim. lapsesi) kontrolloimiseksi tai vahingoittamiseksi?	Kyllä/mahdollisesti Ei Ei tietoa	
2. Onko väkivallan tekijä lähettänyt, tehnyt tai soittanut sinulle tai läheisellesi uhkaavia / väkivaltaisia viestejä, some-päivityksiä tai puheluja?	Kyllä/mahdollisesti Ei Ei tietoa	
3. Tiedätkö tai uskotko, että väkivallan tekijällä on pääsy sinun tai läheisesi digitaalisiin laitteisiin, käyttäjätileihin tai tiedostoihisi tahtomattasi? (esim. puhelin, sähköposti, Facebook, WhatsApp, verkkopankkitunnukset, Find my phone, kuvatiedostot, Google)	Kyllä/mahdollisesti Ei Ei tietoa	
4. Tiedätkö tai uskotko, että väkivallan tekijä seuraa sinun tai läheisesi liikkumista tai tekemisiä teknologian avulla? (esimerkiksi älylaitteiden, vakoiluohjelmien, paikannuslaitteiden tai sijaintitietojen avulla)	Kyllä/mahdollisesti Ei Ei tietoa	

3.8.2021

Täsmentäviä kysymyksiä digitaaliseen väkivaltaan liittyen

Asiakkaan tilanne ja huolet	**Työntekijän muistiinpanoja**
Onko tapahtunut jotain, mikä herättää sinussa erityistä huolta?	
Mitkä asiat huolestuttavat sinua eniten tällä hetkellä?	
Mitä laitteita, sovelluksia ja/tai tilejä sinulla (ja läheisilläsi kuten lapsillasi) on tällä hetkellä käytössä?	
Käytätkö tällä hetkellä väkivallan tekijältä saatuja tai yhteiskäytössänne 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 tms.)?	
Väkivallan tekijän pääsy asiakkaan laitteisiin ja tileihin	**Työntekijän muistiinpanoja**
Epäiletkö tai tiedätkö väkivallan tekijän saaneen selville sinun käyttäjätunnuksen ja salasanan esimerkiksi sähköpostiin, johonkin laitteelle tai sosiaalisen median tilille (esim. Facebook, Instagram, Snapchat)?	
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 tekemiä?	
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 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? (puheluja estetty)	
Ovatko sinun laite/laitteet, sähköposti tai sosiaalisen median tilit olleet tai ovat edelleen väkivallan tekijän hallussa?	
Onko sinulla laitteissasi sovelluksia tai ohjelmia, joita tiedät tai uskot väkivallan tekijän asentaneen?	
Onko käytössäsi älylaitteita, joiden etäkäyttötunnukset ovat tekijän tiedossa?	
Asiakkaan seuraaminen teknologian avulla	**Työntekijän muistiinpanoja**
Tietääkö tekijä sinun olinpaikan (menneen, nykyisen tai tulevan) vaikka ei pitäisi?	
Onko laitteessasi tai mobiilisovelluksessa laitettu sijainnin jakaminen päälle?	
Onko käytössäsi älylaitteita, joita et ole itse asentanut (esimerkiksi navigaattori, eläinten tutkapannat, älykodinkoneet)?	
Onko sinun tietojasi yritetty hankkia muiden henkilöiden kautta digitaalisin välinein?	

3.8.2021

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 kuten turvakodin asiakastietokoneella.

Osa alla olevista toimenpiteistä on normaalia turvakotityötä, osa toimia, joita voidaan tehdä turvakodissa ja osa tulee tehdä yhteistyökumppaneiden kanssa.

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 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

- ➢ Tällöin internet-tilille pääsy edellyttää, että henkilö todistaa kaksi kertaa olevansa hän.