



DeStalk

detect and stop stalkerware and
cyberviolence against women

Juhendmaterjal kübervägivallast ohvritega töötavatele spetsialistidele

 **Blanquerna**
UNIVERSITAT RAMON LLULL

 **UNA CASA
PER L'UOMO**
società cooperativa sociale

kaspersky


WMP // EUROPEAN NETWORK



REGIONE DEL VENETO

Supported by the Rights, Equality
and Citizenship Programme of the
European Union (2014–2020)



Sisu

Kübervägivallaga seotud mõisted	2
Küberjälitamine	3
Küberahistamine	4
Intiimse sisu loata jagamine	5
Tehnoloogiale juurdepääsu piiramine	6
Muud viisid	6
Kübervägivald ja jälitustarkvara: juhised ohvritega töötavatele spetsialistidele	7
Hindamine	7
IT-turvalisuse plaan	8
Riskide tuvastamise elemendid	10
Turvameetmed	11
Kontrollige, kas seadmes on jälitustarkvara	12
Turvameetmed juhuks, kui on kahtlus , et ohvrit jälgitakse ja/või jälitatakse	13
Turvameetmed juhuks, kui on kindel , et telefoni/seadet jälitatakse	14
Mida teha küberahistamise või fotode või teabe loata jagamise korral	15
Sisu eemaldamine täiskasvanutele mõeldud veebilehtedelt	16
Kübervägivald ja jälitustarkvara: tehnoloogia ja sotsiaalmeedia turvalise kasutamisega seotud nõuanded ohvritele	17
Kontrollnimekiri ohvritega töötavatele spetsialistidele	19
Nutitelefonide või muude seadmetega seotud tehnilised ohumärgid	20
Seadmete ja kontode kasutamisega seotud ohumärgid	21
Partneri/toimepanija käitumisega seotud ohumärgid	22
Sotsiaalmeediaga seotud ohumärgid	23
Abivõimalused	23

Juhendmaterjali on koostanud Una Casa per l'Uomo 2022. aasta oktoobris Euroopa Liidu rahastatud projekti „DeStalk: Detect and Stop Stalkerware and Cyberviolence Against Women“ (REC 101005527) raames.

Projekti veebileht: <https://www.work-with-perpetrators.eu/destalk>

Elena Gajotto elena.gajotto@unacasaperluomo.it

Berta Vall Castelló bertavc@blanquerna.url.edu

Dimitra Mintsidis d.mintsidis@work-with-perpetrators.eu

Materjali tõlge eesti keelde on rahastatud Euroopa Majanduspiirkonna ja Norra finantsmehhanismi 2014-2021 programmi „Kohalik areng ja vaesuse vähendamine“ projekti „Ohvriabi süsteemi arendamine“ vahenditest.

Kübervägivallaga seotud mõisted

Kuigi tehnoloogia on olnud meie elu oluline osa juba pikemat aega, on spetsialistid ja poliitikakujundajad hakanud kübervägivallale alles hiljuti rohkem tähelepanu pöörama. Euroopa Liidu tasandil esitas esimese kübervägivalla definitsiooni 2021. aasta novembris Istanbuli konventsiooni rakendamise üle järelevalvet teostav GREVIO:

Naistevastase vägivalla digitaalne mõõde hõlmab mitmesuguseid internetis või tehnoloogiliste vahendite abil toimepandud tegusid, mis on osa vägivalla ringist, mida naised ja tüdrukud oma soo tõttu kogevad (sealhulgas kodus). Sellest tulenevalt on kübervägivald päriselus kogetava soolise vägivalla väljendus internetis ja sellega võrdset kahjulik.

GREVIO üldine soovitus nr 1 naistevastase vägivalla digitaalse mõõde kohta

Selle määratluse kohaselt on kübervägivald naistevastase vägivalla digitaalne mõõde, mis hõlmab internetis või digiseadmete kaudu toimepandud väärkohtlemist.

Oluline on mõista, et alljärgnev kübervägivalla vormide nimekiri ei ole ammendav, sest digitehnoloogia pideva ja kiire arengu tuules muutuvad ja täienevad ka kübervägivalla vormid. Samuti võib sama kübervägivalla vorm paista erinev, nii et eri vormidele iseloomulikud omadused võivad kattuda. Lisaks võib sama vägivallavorm kanda erinevaid nimesid. Nagu Euroopa Soolise Võrdõiguslikkuse Instituut (EIGE) 2017. aastal märkis, oleks kasulik mõistetes poliitilisel tasandil kokku leppida, kuna see võimaldaks organisatsioonidel (nt ohvreid abistavad organisatsioonid, toimepanijatele suunatud programmid ja õiguskaitseasutused) omavahel paremini koostööd teha.

Kübervägivald on katustermin, mis hõlmab kõiki info- ja kommunikatsioonitehnoloogia (IKT) kaudu toimepandud vägivallavorme. Kõige levinumad kübervägivalla vormid on küberjälitamine, küberkiusamine, küberahistamine ja fotode loata jagamine. Nagu GREVIO oma soovituses märgib, võimendab ja hõlbustab tehnoloogia naiste- ja tüdrukutevastase vägivalla vormide rakendamist, ning see on viinud selle nähtuse enneolematu eskaleerumiseni. Internetis või IKT kaudu toimepandud vägivald jätkab päriselus aset leidvat vägivalda ega seisa sellest eraldi – tihti järgib see veebivälise vägivallaga samu mustreid ning toob naiste ja tüdrukute jaoks kaasa psühholoogilisi, sotsiaalseid ja majanduslikke tagajärgi.

Nagu EIGE on täpsustanud¹, hõlmab naiste- ja tüdrukutevastane kübervägivald erinevaid vägivallavorme, mis pannakse toime IKT-vahenditega ohvri soo tõttu või ohvri soo ja muude tegurite (nt rass, vanus, puue, seksuaalsus, elukutse või isiklikud tõekspidamised) kombinatsiooni tõttu.

Igasugune kübervägivald võib:

- a. saada alguse internetis ja jätkuda väljaspool interneti, näiteks töökohal, koolis või kodus;
- b. saada alguse väljaspool interneti ja jätkuda internetis eri platvormide, näiteks sotsiaalmeedia, e-kirjade või kiirsõnumirakenduste kaudu;
- c. olla toime pandud anonüümse ja/või ohvrile tundmatu isiku või isikute rühma poolt;
- d. olla toime pandud ohvrile tuntud isiku või inimeste rühma poolt, näiteks (endine) partner, koolikaaslane või kolleeg.

IKT-vahendite paljususe tõttu on soopõhist kübervägivalda võimalik toime panna paljudes eri vormides. Järgnevalt on esitatud **nimekiri peamistest viisidest, kuidas soolist kübervägivalda toime pannakse.**

Küberjälitamine* hõlmab tahtlikke korduvaid tegusid. Küberjälitamise puhul kasutatakse IKT-vahendeid, et ahistada, hirmutada, taga kiusata, nuhkida või luua soovimatu suhtlus või kontakt. Selline kahjustav käitumine tekitab ohvris ohu- või ebaturvalisuse tunnet või stressi². Internetis jälitamiseks võib kasutada erinevaid viise:

- ⇒ **jälitustarkvara:** ohvri seadmesse paigaldatakse salaja rakendused, mille abil saab teda jälgida ja jälitada;
- ⇒ **hääkimine või krakkimine:** juurdepääs internetis (nt pilves) või isiklikus arvutis salvestatud suhtlusele ja andmetele ilma omaniku nõusolekuta. See hõlmab veebikaamera hääkimist, mis sageli mõjutab naisi, ja nutikodu seadmete kasutamist vestluste pealtkuulamiseks;
- ⇒ **küberjälgimine:** IKT kasutamine selleks, et jälgida ohvri tegevust, asukohta ja sotsiaalset suhtlust. Seda saab teha spetsiaalsete seadmete (GPS-jälgimisseadmed, aktiivsusmonitorid jne) või veebikontodele juurdepääsu kaudu (Google või iCloud jne).

* EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV (EL) 2024/1385 (2024): **küberjälitamine** on tänapäevane vägivallavorm, mida sageli pannakse toime pereliikmete või samas leibkonnas elavate isikute vastu, kuid mida panevad toime ka endised partnerid või tuttavad. Tavaliselt kuritarvitab süüteo toimepanija tehnoloogiat, et intensiivistada oma surveavat ja kontrollivat käitumist, manipuleerimist ja jälgimist, mis omakorda suurendab ohvri hirmu ja ärevust ning isoleerib ta järk-järgult sõpradest, perekonnast ja tööst.

¹ EIGE (2022) Cyber Violence against Women and Girls. Key terms and Concepts (europa.eu)

² Ibid

- ⇒ ohvri **jälgimine internetis**: tema sotsiaalmeediakontode jälgimine, kõigile tema postitustele vastamine, samade gruppidega liitumine ja tema pealetükkiv märgistamine (täägimine). Seda saab teha ka võltskontodega.

Küberahistamine* on lai kategooria, mille alla kuuluvad ähvardused või muu ründav käitumine isiku või isikute rühma poolt, mille eesmärk on teist isikut digitaalsete avalike ja erakanalite kaudu solvata, häbistada või halvustada. Küberahistamine hõlmab järgmist:

- ⇒ soovimatud e-kirjad või sõnumid;
- ⇒ solvavad või sobimatud päringud sotsiaalmeedias või internetivestlustes;
- ⇒ e-kirjade, sõnumite või vestluste kaudu edastatud füüsilise või seksuaalse vägivalla ähvardused;
- ⇒ vihakõne, s.o solvava, mustava või ähvardava keele kasutamine internetis;
- ⇒ sobimatud või seksuaalsed kommentaarid sotsiaalmeediapostituste või seal leiduva muu infosisu kohta.

Küberahistamise hulka kuuluvad muu hulgas järgmised tegevused.

- ⇒ **Laimamine** (*slandering*) tähendab kellegi maine kahjustamist tema kohta valeinfo jagamise kaudu (nt kuulujuttude levitamine sotsiaalmeedias).
- ⇒ **Libustamine** (*slut-shaming*) on CYBERSafe'i (2020) järgi internetis „inimeste, eriti naiste ja tüdrukute kritiseerimine, kelle käitumist ja välimust ei peeta seksuaalsusega seotud küsimustes kehtivatele ootustele vastavaks“.
- ⇒ Vägistamise, väärkohtlemise või surmaga **ähvardamine internetis** (*online threats*).
- ⇒ **Keha häbistavad sõnumid või kommentaarid** (*body shaming*), mille kirjutamise eesmärk on alandada inimest, tehes tema kehakuju või suuruse kohta pilkavaid või kriitilisi märkusi.
- ⇒ **Sooline trollimine** (*gendertrolling*) tähendab internetis toimepandavaid pahatahtlikke tegusid, mis hõlmavad provokatiivsete e-kirjade või sotsiaalmeediapostituste, sh vägistamis- ja tapmisähvarduste saatmist või avaldamist. Sarnaselt trollimisega on ka soolise trollimise eesmärk tekitada vaidlusi ja suurendada jälgimist, õhutades oma sihtmärki vihaselt või ärritunult vastama³.

* EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV (EL) 2024/1385 (2024): **küberahistamine** on korduv või pidev ähvardav käitumine IKT vahendite abil, mis on suunatud isiku vastu, vähemalt juhul, kui selline käitumine hõlmab ähvardusi panna toime kuritegu, ja mis tõenäoliselt põhjustab kõnealuses isikus tõsist hirmu iseenda või oma ülalpeetavate turvalisuse pärast

³ EIGE (2022) Cyber Violence against Women and Girls. Key terms and Concepts (europa.eu)

⇒ **Seksuaalse sisuga siivutud ettepanekud** (*sexual solicitation*) ehk soovimatud ettepanekud rääkida seksist või teha seksuaalseid tegevusi mitmesugustes internetikontekstides, näiteks seksuaalselt ühemõtteliste piltide saatmine või tehnoloogia kaudu seksuaalses suhtluses osalemine. See võib viia pahatahtlike misogynüünsete kommentaaride, ahistamise ja ähvardusteni, eriti kui ohver on ettepanekud mingil viisil tagasi lükanud⁴.

Intiimse sisu loata jagamine hõlmab mitmesuguseid meetodeid, mille ühisnimetajaks on ilma isiku nõusolekuta jagatud või omandatud intiimse sisuga pildid või videod. See hõlmab järgmisi tegevusi.

⇒ **Seksuaalne väljapressimine** (*sextortion*) on ähvardus avaldada intiimse sisuga materjale (pildid, videod, süvavõltsingud ehk *deepfake*'id, intiimse sisuga kuulujutud), kui naine ei anna toimepanijale üle täiendavat intiimse sisuga materjali või raha või mõnikord ka mõlemat. Toimepanija võib olla endine partner, kes sai pildid või videod oma käsutusse suhte ajal ning kes soovib ohvrit avalikult häbistada ja alandada, tihti selleks, et maksta kätte suhte lõpetamise eest⁵.

⇒ **Intiimsete piltide ja/või videote loata jagamine** on ähvardus jagada IKT kaudu ohvrist tehtud intiimseid, isiklike ja/või manipuleeritud pilte ja/või videoid või selliste piltide/videote jagamine ilma ohvri loata. Loa puudumine võib tähendada, et pildid/videod on omandatud ohvri loata, neid on ohvri loata manipuleeritud või on omandamiseks luba küll olemas, ent puudub ohvri luba nende jagamiseks. Sellist teguviisi nimetatakse üldiselt kättemaksupornoks, ent see pole sisuliselt õige, kuna loob mulje, justkui oleks tegemist toimepanija reaktsiooniga ohvri etteheidetavale tegevusele, mis võib viia ohvrisüüdistamiseni⁶.

⇒ **Naise intiimsetest kehaosadest loata piltide või videote tegemine** (*creepshot voyeurism*), sealhulgas dekolteesse ja seeliku alla vaatamine, tähendab partneri või mõne teise (võõra) naise intiimsetest kehaosadest (nt tagumik, jalad või dekoltee) piltide või videote tegemist ilma isiku nõusolekuta. Seda võidakse teha peidetud kaameraga või olukorras, kus naine seda ei märka (on duši all, magab jne).

⇒ **Süvavõltsing** (*deepfake*) on tehisintellekti abil valmistatud töödeldud või sünteetiline heli- või visuaalmeedia, mis näib autentsena ja milles esinevad inimesed, kes näivad ütlevat või tegevat midagi, mida nad ei ole päriselus kunagi öelnud või teinud. Enamik süvavõltsinguid naistest ja tüdrukutest kujutab intiimseid pilte või seksuaaltegevusi ning neid jagatakse platvormidel või

⁴ EIGE (2022) Cyber Violence against Women and Girls. Key terms and Concepts (europa.eu)

⁵ *Ibid*

⁶ *Ibid*

täiskasvanutele mõeldud „meelelahutuslikel“ veebilehtedel ilma neil kujutatud naiste ja tüdrukute loata.

- ⇒ **Küberliputamine** (*cyberflashing*) on soovimatute intiimse sisuga piltide saatmine, peamiselt meeste suguelunditest (*dick pics*) tutvumis- või sõnumirakenduste või tekstisõnumite kaudu või näiteks Airdropi või Bluetoothi kasutades.

Tehnoloogiale juurdepääsu piiramine

Ajal, mil paljusid igapäevategevusi tehakse seadmete ja rakenduste abil, on tehnoloogiale juurdepääsu piiramisel või keelamisel ohvri elule tohutu mõju. See on viis teda kontrollida või isoleerida. Näiteks takistab terviserakendustele juurdepääsu piiramine tervise eest hoolitsemist. Samamoodi takistab juurdepääsu piiramine pangarakendustele naise võimalust kasutada oma raha, piirates seeläbi tema iseseisvust. Lisaks võivad seadmete või ühenduste kasutamise piirangud takistada naisel abi otsimast.

Juurdepääsu tehnoloogiale võidakse piirata järgmiselt:

- ⇒ seadme või konto kasutamise piiramine, funktsioonide (nt kaamera, mikrofon jne) kasutamise piiramine või selle kasutamise aja kontrollimine;
- ⇒ seadme kahjustamine või selle kasutuskõlbmatuks muutmine;
- ⇒ internetiühenduse tõkestamine;
- ⇒ paroolide ja seadete muutmine.

Muud viisid

Doksimine (*doxing* või *doxxing*) on isiku äratuntavate ja sageli isiklike andmete (nimi, telefoninumber, e-posti aadress, kodune aadress jne) jagamine veebiplatvormidel ilma isiku loata. Kuna avaldatud teave võimaldab tavaliselt kindlaks teha ohvri füüsilise asukoha, võib *doxing* kuulutada ette veebivälise vägivalda toimepanemist. Sageli toimub *doxing* paarisuhtevägivalda raames⁷.

- **Teise isiku identiteedi ebaseaduslik kasutamine (identiteedivargus)** tähendab kellegi isikuandmete kasutamist selleks, et teeselda selleks isikuks olemist ja omandada tema nimel raha või kaupu. Paljud tasuta rakendused võimaldavad ka helistaja identiteedi varjamiseks kõne vastuvõtja ekraanile ilmuva helistaja ID võltsimist (*spoofing*).
- Inimkaubandus mis on vahendatud läbi interneti, sotsiaalmeedia ja tehnoloogiliste seadmete.

⁷ EIGE (2022) Cyber Violence against Women and Girls. Key terms and Concepts (europa.eu)

Kübervägivald ja jälitustarkvara: juhised ohvritega töötavatele spetsialistidele

Kübervägivald on katustermin, mis viitab internetis toimepandud soolise vägivalla erinevatele tüüpidele ja vormidele ning mille võib laias laastus jagada järgmistesse rühmadesse: küberjälitamine (jälitustarkvara või muude IKT-vahendite abil), kujutisi kasutav seksuaalne väärkohtlemine (loata piltide ja/või videote jagamine, *sextortion* jne) ja küberahistamine (küberkiusamine, laimamine, ähvardamine internetis jne). Kübervägivald võib toimuda tavapäraselt päriselus toimepandavate vägivallavormide internetti laienemise teel (näiteks küberahistamine või küberjälitamine). Kuid IKT on viinud ka uute vägivallavormide tekkimiseni (näiteks loata intiimsete piltidega seotud väärkohtlemised või *doxing*), mis võivad kahju ulatust võimendada.

Kübervägivalda saab toime panna erinevate seadmete kaudu (nutitelefonid, arvutid, tahvelarvutid, GPS-seadmed, nutikodu seadmed jne) ja mitmesugustel veebiplatvormidel (sotsiaalmeedia, veebilehed, sõnumirakendused, isiklikud kontod jne) – kõik need seadmed ja platvormid arenevad pidevalt, pakkudes kuritarvitajatele uusi võimalusi uute vägivallavormide kasutamiseks. Samuti loob seadmete ja platvormide mitmekesisus võimalusi erinevat tüüpi toimepanijatele, kes võivad olla nii ohvrile teada (näiteks (endine) partner, koolikaaslane, kolleeg, sõber jt) või talle tundmatud üksikisikud või isikute rühmad.

Nagu me teame, on digiruum internetis ja füüsilise ruumi väljaspool internetti omavahel tugevalt seotud ning kübervägivald peegeldab tihti füüsilises maailmas toimepandavaid väärkohtlemise ja ohvrustamise vorme või eelneb neile⁸.

Seetõttu peavad ohvritega töötavad spetsialistid kübervägivalla võimalikkust põhjalikult hindama ja arvestama turvalisuse plaani koostamisel ka IT-turvalisuse elemente.

Hindamine

Hindamine aitab meid olemasolevate kübervägivalla vormide tuvastamisel, ohvrite nõustamisel, turvalisuse plaani väljatöötamisel ning dokumentide ja tõendite kogumisel.

⁸ EIGE (2022) Cyber Violence against Women and Girls. Key terms and Concepts (europa.eu)

Kübervägivald võib tunduda kõikehõlmav, sest seda võidakse toime panna igal ajal, igal pool ja mitmel erineval viisil. Hindamine annab ohvrile kindlustunde, et nende kogemus on tõeline ja kahjustav. Ohvritega töötades on oluline pidada silmas kõiki kübervägivalla vorme ja teada, kuidas neist igaühega tegeleda.

Kübervägivalla hindamise raamistik

Kübervägivalla hindamisel tuleb järgida järgmisi samme.

- Kuulake ohvri kogemust
 - Mis juhtus ja kui sageli?
 - Kuidas see ohvri arvates juhtus?
- Hinnake, millist teavet kuritarvitati
 - Millist teavet oli toimepanijal juhtunu põhjustamiseks vaja?
 - Kus seda teavet hoitakse? Kellel ja kuidas on sellele juurdepääs?
- Koostage nimekiri seadmetest ja kontodest, pidades silmas, millist tüüpi teavet toimepanija kasutas
- Hinnake juurdepääsetavust
 - Millistele kontodele ja seadmetele pääseb juurde ohver ja millistele toimepanija?
 - Kuidas tagada nende kontode või seadmete turvalisus?
- Hinnake riske
 - Mõelge, mida on võimalik turvaliselt teha.
- Planeerige järgmisi samme
 - Mis on ohvri eesmärgid?
 - Kuidas neid turvaliselt saavutada?
 - Kuidas turvaliselt tõendeid koguda?

IT-turvalisuse plaan

IT-turvalisuse plaan ei erine teistest turvalisuse plaanidest, mida ohvritega tegelevad spetsialistid tavaliselt kasutavad. Oluline on keskenduda ohvri vajadustele ja eesmärkidele nii lühemas kui ka pikemas perspektiivis ning mõista, kuidas kübervägivald tema elu mõjutab. Tehnilised teadmised on turvalisuse planeerimise juures abiks, kuid mitte hädavajalikud.

Hea turvalisuse plaan on personaalne, ohvrile lähtuv ja teda võimestav. Pidage meeles, et see, mida turvalisus ohvri jaoks tähendab võib kiiresti muutuda. Turvalisuse plaani läbimõtlemine tähendab, et

ohvriks antakse vahendid ja strateegiad oma riskide ja turvalisuse juhtimiseks, et seeläbi osa kontrollist endale n-ö tagasi võita.

Nagu eespool mainitud, tuleb turvalisuse plaani läbimõttlemisel arvestada ohvri lühi- ja pikaajaliste vajaduste ja eesmärkidega.

- Vastutusele võtmine ja õigusküsimused
 - o Dokumentide ja tõendite kogumine kohtumenetluseks
 - o Toimepanija vastutusele võtmine ja meetmed, mis ohvrit toimepanija eest kaitsevad
 - o Tsiviilõiguslikud kaitsevahendid: abielulahutus, laste hooldusõigus
- Suurem privaatsus ja tehnoloogiline turvalisus
 - o Turvalise ühenduse loomine toimepanijaga
 - o Olemasolevate sotsiaalmeediaprofiilide turvalisuse suurendamine
 - o Uute kontode ja profiilide loomine
- Vägivalla peatamine
 - o Arusaam sellest, kuidas kübervägivalda toime pannakse
 - o Võimaluste leidmine väärkohtlemise leevendamiseks
 - o Tehnoloogilise lahenduse leidmine väärkohtlemise vähendamiseks või ennetamiseks

IT-turvalisuse plaani alustalad

Üks olulisemaid aspekte, millega tuleb arvestada, on väärkohtlemise dokumenteerimine. Ohvrid tuleb teavitada ja juhendada, kuidas

- pidada toimuva kohta päevikut,
- teha kuvatõmmiseid või pilte,
- hoida alles originaale (e-kirjad, sõnumid, kõnepostiteated või rakendused),
- säilitada olulisi dokumente turvalistes kohtades või spetsiaalsetes salvestusrakendustes.

Teine oluline aspekt on uurida, kes seadmetele ja kontodele juurde pääsevad ning neid kontrollivad.

Selleks tuleb hinnata järgmist:

- mil viisil ohver suhtleb,
- millised seadmed tal on,
- kuidas ta ringi liigub,
- milline on internetis kättesaadav isikut tuvastav teave (*Personally Identifiable Information* ehk PII).

Riskide tuvastamise elemendid

Võimalike riskiallikate hindamisel on oluline meeles pidada, et isikuandmeid saab salvestada ja „meelde jätta“ erinevates toimepanija poolt juurdepääsetavates seadmetes, rakendustes ja kontodel, näiteks:

- sotsiaalvõrgustikud (Facebook, Instagram, TikTok jne)
- Paypal, Wise või muud elektroonilised maksesüsteemid
- pangandus
- terviserakendused
- Amazon (sh Prime Video)
- kaupluste jms kliendikaartidega seotud rakendused
- toidukulleri rakendused (Wolt, Bolt, UberEats jne)
- Spotify, YouTube
- voogedastusrakendused (Netflix, Discovery+, Disney+, DAZN)
- treeningrakendused (Garmin, Fitbit, MiFit, Strava, Run Keeper jne)
- reisirakendused (Booking, Trivago, TripAdvisor jne)
- tutvumisrakendused (Tinder, Bumble jne)
- asukoha jagamise ja jälgimise rakendused (Find My Friends jne)

Ühenduste, teabe ja juurdepääsu puhul tuleb arvestada järgmisi aspekte.

Ühendus

- Millega on seadmed ühendatud (sh muud seadmed, kontod, rakendused)?
- Kuidas on ühendus loodud (Wi-Fi, Bluetooth, Airdrop jm jagamisfunktsioonid, juhtmega ühendus)?
- Kes ühendust kontrollib?

Teave

- Millist teavet jagatakse?
- Kellele seda teavet jagatakse (teine seade, veebikonto jm)?
- Kas ettevõttel on privaatsuspoliitika?
- Kas seda, mida ja kellega jagatakse, on võimalik piirata?

Juurdepääs

- Kuidas seadmele juurde pääseb (kaugjuurdepääs, füüsiline juurdepääs)?
- Millised kontod on seotud?
- Kellel on juurdepääs?

Et tehnoloogia kuritarvitamise hindamist ja IT-turvalisuse plaani läbimõtetmist hõlbustada, on võimalik kasutada selle juhendmaterjali lisas olevat kontrollnimekirja. See sisaldab ohumärke, mis aitavad kübervägivalda võimalikke vorme tuvastada, ning viiteid nendega seotud riskidele ja vastumeetmetele.

Turvameetmed

Kui eksisteerib võimalus, et toimepanija jälgib ja jälitab ohvri telefoni, on esmatähtis töötada koos ohvriga välja selge ja põhjalik **IT-turvalisuse plaan**. Seejuures tuleb alati silmas pidada, et **järsud muudatused võivad toimepanija vägivaldset käitumist eskaleerida**.

IT-turvalisuse plaan peaks käsitlema järgmisi teemasid.

- **Turvaline suhtluskanal**

Kui telefoni jälitatakse, **ärge** loobuge sellest ega kustutage sellest kahtlasi rakendusi. Uurige, kas ohvril on võimalik osta uus seade või seda laenata – mõlemal juhul tuleb kasutada uut SIM-kaarti. Teine võimalus on kontrollida, kas ohvril on võimalik kasutada mõne usaldusväärse isiku seadet või avalikku arvutit (näiteks raamatukogus).

- **Turvalise seadme kasutamine**

Otsustage, kuhu võiks ohver turvalise seadme peita ja millal/kuidas seda kasutada. Ohver peaks turvalist seadet kasutama kõigi nende vestluste jaoks, millest toimepanija ei tohi midagi teada (nt suhtlus ohvriabiteenuste osutajatega, juristi, politsei, arstiga jne). Muudeks tavapäraseks tegevusteks peaks ta jätkuvalt kasutama jälitatavat telefoni, et toimepanija ei hakkaks kahtlustama ning et ohvril oleks võimalik koguda tõendeid. Rääkige ohvriga sellest, kui oluline on turvalist seadet oma laste eest salajas hoida.

- **Veebisuhtlus- ja sotsiaalmeediakontode kasutamine**

Vajaduse korral looge turvalised e-posti aadressid ja pilvsalvestusruumi kontod, et usaldusväärsete adressaatidega turvaliselt suhelda ning salvestada olulisi dokumente ja tõendeid. Rääkige naisega sellest, mis liiki teavet on mõistlik sotsiaalmeedias jagada.

Turvaplaani koostamisel tuleb läbi mõelda ka see, millised turvaprobleemid või piirangud kaasnevad ohvri jaoks telefoni väljalülitamisega. Seega tuleb läbi arutada, milline võib olla toimepanija reaktsioon, kui ta üritab ohvrile helistada ja tema telefon on välja lülitatud. Mõned ohvrid teavad, et nad peavad selle kohta hiljem aru andma ja see võib vägivalda riski suurendada. Selgitamine, kui kaua politsei toimingud aega võivad võtta, ja info selle kohta, kas toimepanija helistab alati kindlal kellaajal, võib

osutada väga kasulikuks teabeks, mis aitab ohvri teha teadlikke valikuid selle kohta, kas, kuidas ja millal telefon välja lülitada.

Turvaplaani väljatöötamisel tuleb mõelda ka sellele, kas ohvri on tema turvalisuse seisukohalt oluliste tegevuste jaoks tingimata telefoni vaja. Näiteks, kas ta teab täpselt, kuhu ta läheb, või on tal vaja kasutada kaarti. Kas telefonis on tõendeid, mida ta tahab politseile ülekuulamise ajal näidata? Seetõttu tuleb läbi mõelda kõik, mis võib viia selleni, et ohvri tekib vajadus telefon sisse lülitada. Seejärel saab ta kavandada tõendite kogumist viisil, mis võimaldab kogutut näidata ka siis, kui telefon on välja lülitatud.

Samuti tuleb selgeks teha, kui kiiresti telefon oma asukohta uuendab, et naine ei lülitaks lahkudes oma telefoni sisse kohe parklas, vaid ootaks, kuni ta on sihtkohast veidi kaugemale jõudnud.

Kontrollige, kas seadmes on jälitustarkvara

Kui teie poole pöördunud naisel on kahtlus, et tema (endine) partner teab temast liiga palju, ilma et naine ise oleks temaga sellist teavet jaganud, pakkuge naisele võimalust seade koos temaga üle kontrollida.

Seadme ülekontrollimiseks on mitmeid viise, kusjuures kõigiga neist kaasnevad omad riskid.

- ⇒ Ohumärkide kontrollimine (vt ohumärkide tabelit) on kõige vähem sekkuv viis ja seda tuleks teha alati, kuid see annab ka kõige vähem kindlust.
- ⇒ Viirusetõrjeprogrammi kasutamine mobiilseadmetes. Pidage meeles, et jälitustarkvara võib toimepanijale viirusetõrjeprogrammi kasutamisest märku anda.
- ⇒ Spetsiifiliste tööriistade (näiteks [TinyChecki](#)) kasutamine. Toimepanija ei saa selle tööriista kasutamisest teada, kuid selleks on vaja teist ettevalmistatud seadet.

PIDAGE MEELES: kui otsite seadmest tundmatuid rakendusi, siis ärge unustage, et operatsioonisüsteem installib vaikimisi mitmeid rakendusi, mis võivad teile tundmatud olla. Kahtluse korral küsige tundmatute rakenduste tuvastamiseks abi usaldusväärse IT-tehnikult.

Ohvrite abistamisega tegelev organisatsioon saab oma spetsialiste seadmete kontrollimise alal koolitada ja tutvustada neile kontrollimisvahendeid nagu TinyCheck.

Teine võimalus on teha koostööd usaldusväärse IT-tehnikuga, kes ohvrite seadmed üle vaatab.

PIDAGE MEELES: kui kontrolli käigus midagi kahtlast ei tuvastatud, ei tähenda see, et probleemi pole. Toimepanija võib kasutada ohvri jälgimiseks/jälitamiseks muid vahendeid – näiteks võib tal olla juurdepääs ohvri veebikontodele või ta võib kontrollida ohvri telefoni, kui ta jätab selle järelevalveta jne.

Turvameetmed juhuks, kui on **kahtlus**, et ohvrit jälgitakse ja/või jälitatakse

- ⇒ Teavitage ohvrit, et jälitustarkvara võib tema vestlusi salvestada isegi siis, kui seade on välja lülitatud. Soovitage talle, et ta jätaks seadme autosse või ei võtaks seda endaga kaasa, kui ta vestleb ohvriabiteenuse osutaja, arsti, politsei, juristi või mõne muu abistajaga.
- ⇒ Kui ohver on telefoni hiljuti kingiks saanud, taastage telefoni tehaseseaded. Mõne jälitustarkvara puhul ei pruugi see töötada, kuid enamasti õnnestub jälitustarkvara eemaldada. Arvestage, et toimepanija saab sellest teada, kuna ta ei saa enam seadet jälgida.
- ⇒ Kontrollige, kas interneti andmekasutus on põhjusega suurenenud (selle jälgimiseks on võimalik tulevikus ka rakendusi installida).
- ⇒ Installige viirusetõrjerakendus (NB! Jälitustarkvara rakendused võivad toimepanijat viirusetõrje installimisest teavitada).
- ⇒ Vahetage sageli seadmete ja kontode paroole ning kasutage paroole, mida ei ole lihtne ära arvata.
- ⇒ Muutke telefoni lukust avamise meetodit. Kasutage sõrmejälje ja näotuvastuse asemel PIN-koodi või mustrit.
- ⇒ Kontrollige, kas rakendustele on antud asukoha ja kaamera õigused, ning tühistage need, kui need on aktiivsed.
- ⇒ Ühendage WhatsApp Web, Messenger, Viber ja muud sarnased kontod arvutitest ja muudest toimepanijale juurdepääsetavatest seadmetest lahti.
- ⇒ Rääkige ohvriga sellest, kui oluline on mitte lasta oma lastel oma seadmeid kasutada.
- ⇒ Muutke internetipanga sisselogimisandmeid.
- ⇒ Paluge usaldusväärsel mehaanikul auto GPS-i kontrollida ja võimaluse korral see desaktiveerida.
- ⇒ Soovitage võõraste sõbra- ja jälgimiskutseid mitte vastu võtta.
- ⇒ Vaadake üle jälgijate/sõprade loend igal sotsiaalmeediaplatvormil ning soovitage mitte jälgida tundmatuid isikuid ja olla nendega sõber. Pidage meeles, et kui profiil/konto on avalik, näevad selle sisu kõik, isegi kui ta ei ole jälgija/sõber.

- ⇒ Soovitage ohvril mitte jagada sotsiaalmeedias ja WhatsAppis stoorisid, pilte ega muid üksikasju, mis võivad anda teavet tema asukoha kohta.
- ⇒ Uurige, kas ohvril võib olla muid pealtnäha süütuid kontosid, mida ta toimepanijaga jagab (vt loendit allpool).

Turvameetmed juhuks, kui on **kindel**, et telefoni/seadet jälitatakse

Kui on kindel, et seadet jälitustarkvara rakenduse kaudu jälitatakse või et toimepanija jälgib ohvrit muude IT-vahendite abil, tuleb rakendada vajalikke meetmeid, et tagada ohvri turvalisus ja koguda toimepanija vastu tõendeid.

- ⇒ Jälitustarkvara tuvastamise korral on tavapärane, et ohver soovib sellest kohe lahti saada. Selgitage talle selle eemaldamise tagajärgi (vägivalla eskaleerumine, tõendite hävitamine).
- ⇒ Vaadake üle IT-turvalisuse plaan ja vajaduse korral tugevdage seda.
- ⇒ Pidage meeles, et seadme tehaseseadete taastamine hävitab tõendid ega pruugi olla vanemate telefonide puhul efektiivne.
- ⇒ Aidake ohvril aktiveerida uus SIM-kaart ja leida endale turvaline seade.
- ⇒ Rakenduste installimisel uude seadmesse või pärast vana seadme tehaseseadete taastamist laadige rakendused alla otse poest, mitte varukoopiast, sest see võib jälitustarkvara rakenduse uuesti alla laadida.
- ⇒ Looge turvalise seadme jaoks uus Google'i või iCloudi konto.

PIDAGE MEELES: uute Google'i või iCloudi kontode loomine turvalise seadme aktiveerimiseks on IT-turvalisuse plaani oluline samm, sest need kontod annavad juurdepääsu mitmesugustele rakendustele ja teabele nagu e-kirjad, pilvesalvestuse failid, kaardid, asukohad, fotod, kontaktid jne.

- ⇒ Kui jälitustarkvara ei ole, aga toimepanija jälgib ohvrit muude IT-vahendite kaudu (näiteks tal on juurdepääs tema veebikontodele), koguge andmeid selle kohta, milliseid kontosid/andmeid jälgitakse.
- ⇒ Isegi kui ohver ei ole kindel, kas ta soovib politseisse pöörduda, soovitage tal alles hoida juhtumite logi – sealhulgas kuupäev, kellaaeg, asukoht, tunnistajad (kui neid on), tehnoloogia, mille kasutamist kahtlustatakse (nt telefon, e-post jne), ja lühikirjeldus selle kohta, mida toimepanija tegi.
- ⇒ Tuletage ohvrile meelde, et ta muudaks paroole ainult siis, kui see on ohutu.

- ⇒ Rääkige läbi, kuidas kasutada jälgitavat seadet või kontot organiseeritud ja kontrollitud viisil nii, et see väldiks toimepanijale liigse teabe andmist, ent samas ei tekitaks temas kahtlusi.

Mida teha küberahistamise või fotode või teabe loata jagamise korral

Need kübervägivalla vormid, sealhulgas seksuaalne väljapressimine (*sextortion*) ja kättemaksuporno, on paljudes ELi riikides karistatavad ning politseid tuleks teavitada lähtuvalt antud riigi õigusaktidest.

Kui te kahtlustate või olete kindel, et ohvri suhtes tarvitatakse selliseid kübervägivalla vorme, siis saate teda edasise kahju ärahoidmisel ja tõendite kogumisel toetada järgmiste soovitude ja meetmetega.

- ⇒ Oluline on tõsta sotsiaalmeedia kontode privaatsustaset, mis tuleks seada kõrgeimale võimalikule tasemele.
- ⇒ Võimalik on seadistada [Google Alerts](#), et jälgida, kas internetis jagatakse mingit ohvriga seotud sisu. Google annab e-kirjaga märku, kui teatud otsingusõnad (näiteks ohvri nimi) Google'i otsingusse ilmuvad.
- ⇒ Selleks et sotsiaalmeedias ahistamise kohta tõendeid koguda, tuleb kõigepealt teha ahistamisest/väärkohtlemisest kuvatõmmised. Pidage meeles, et kuvatõmmised ei ole kohtus veenvad tõendid ja et hankida tuleb ka digitaalsed tõendid.
- ⇒ Arutage, kas ahistamisest või piltide avaldamisest peaks teavitama sotsiaalmeediaplatformi (lugege läbi konkreetse sotsiaalmeediaplatformi kasutajatingimused: [Facebook](#), [Instagram](#), [X](#), [YouTube](#), [TikTok](#)) või veebilehte haldavat ettevõtet. Kui sisu rikub veebilehe teenuse osutamise või kasutustingimusi, võib lehe haldaja sisu eemaldada. Sellisel juhul on tõendite säilitamiseks oluline väärkohtlemine kõigepealt dokumenteerida. Selle kohta, kuidas täiskasvanutele suunatud veebisait teavitada, saate lugeda altpoolt.
- ⇒ Mõnikord võib sama sisu olla avaldatud rohkem kui ühes kohas. Sel juhul võib aidata otsingumootorite pöördotsingu funktsioon. Pöördotsingu tegemiseks peate laadima pildi otsingumootoris, mis skaneerib veebi, et näha, kas see on kuskil avaldatud. Arvestage, et see protsess ja selle tulemus võib olla ohvri jaoks väga häiriv.
- ⇒ Ahistavaid telefonikõnesid saab salvestada ja tõendusmaterjalina alles hoida.

HOIATUS: kontrollige kindlasti, kas teie riigi eraelu puutumatust käsitlevad õigusaktid lubavad telefonivestluste salvestamist teise osapoole teadmata. Eestis on lubatud salvestada oma vestlusi enda tarbeks, kuid neid ei ole lubatud jagada kolmandate isikutega.

- ⇒ Telefoninumbri või helistaja ID võltsimise (*spoofing*) korral on oluline kõnelogid dokumenteerida, teha helistaja ID-st foto/kuvatõmmis ning registreerida kõnede kuupäev ja kellaaeg ning ka telefonikõned, et näidata algse kõne numbrit, kuupäeva ja kellaaega.
- ⇒ Kui sisu on juba avaldatud, saab selle otsingumootoritest eemaldada: Euroopa Liidu elanikel on õigus nõuda, et lingid lehtedele, mis sisaldavad aegunud, ebaolulisi, ülemääraseid või ebatäpseid andmeid, [Google'i](#) otsingutulemustest eemaldataks. See ei nõua lehtede mahavõtmist, vaid ainult seda, et neid ei näidataks Google'i otsingutulemustes, vähendades nii võimalusi nende leidmiseks. Sama saab taotleda ka [Bingilt](#) ja [Yahoolt](#) (iga riigi jaoks võib olla erinev link).
- ⇒ Kui pildid/videod on juba avaldatud, võib kommentaaride ja tagasiside lugemine mõjuda veelgi häirivamalt kui pildid/videod ise. Soovitage ohvrile, et ta ei jälgiks internetis tema kohta leiduvat sisu ja selle kommentaare.
- ⇒ Kui toimepanija on ähvardanud, et avaldab ohvri jaoks isiklikku sisu Facebookis ja Instagramis, saate aidata ohvril liituda Facekooki [Pilot NCII programmiga](#). See programm võib takistada teatud piltide avaldamist. Selleks peab ohver võtma ühendust mõne Piloti partnerorganisatsiooniga (vt nimekirja [siin](#)) ja esitama blokeerimiseks originaalpildi (mitte kuvatõmmise).

Sisu eemaldamine täiskasvanutele mõeldud veebilehtedelt

Kui isiklik sisu on avaldatud täiskasvanutele mõeldud veebilehel, on enamikul neist olemas eeskirjad sellise sisu eemaldamiseks. Sellistelt veebilehtedelt sisu eemaldamiseks trükkige internetiotsingusse saidinimi *content removal request* (nt xvideos content removal request).

Soovitused turvaliseks teavitamiseks

- Kasutage teavitamisel inkognito režiimi.
- Ärge kasutage isiklikku e-posti aadressi (looge eraldi aadress just selleks otstarbeks).
- Ärge esitage oma isikutunnistuse koopiat, kui veebisaidid seda nõuavad.
- Sisestage selle video või pildi täpne URL, mida soovite eemaldada.
- Taotlege kõigi videote ja piltide, sealhulgas pispiltide eemaldamist.

Kübervägivald ja jälitustarkvara: tehnoloogia ja sotsiaalmeedia turvalise kasutamise seotud nõuanded ohvritele

Tehnoloogia on meie elu lahutamatu osa: see on kõikjal meie ümber ja me kasutame seda pidevalt. Sestap on oluline teada, kuidas oma isiklikku küberturvalisust suurendada, et saaksime jätkuvalt tehnoloogiat kasutada ja selle kaudu teistega ühenduses olla.

Kui elate koos vägivaldse partneriga või olete temast lahku läinud, siis leiate siit mõned nõuanded, kuidas oma digitaalset turvalisust parandada.

Kasutage turvalist seadet – s.o seadet, millele teie partner juurde ei pääse. See võib olla uus seade, avalikult kasutatav seade või usaldusväärselt isikult saadud seade. Kasutage seda seadet kogu sellise teabe ja suhtluse jaoks, millest teie partner ei tohi teada.

See hõlmab suhtlust ohvritega töötavate spetsialistide, politsei, juristi, arsti, maksekeskkondade, pankadega jne. Hea valik on ka vana mobiiltelefon, millel ei ole andmesideühendust.

Aktiveerige uus telefoninumber või kasutage turvalist numbrit, et suhelda politsei, ohvriabiteenuse osutaja ja oma juristiga. Jagage seda uut numbrit ainult usaldusväärsete inimestega.

Lisage seadmetele parool või PIN-kood. Iga teie seadet – telefoni, arvutit või tahvelarvutit – tuleb kaitsta parooli, pääsukoodi või PIN-koodiga, mida teate ainult teie. Ärge kasutage pääsukoodide määramisel sünnipäevi, lemmikloomade nimesid ega midagi muud, mis teile meeldib (toit, filmid, laulud) ja mida on lihtne ära arvata. Ärge kasutage igas seadmes sama pääsukoodi.

Ärge jagage paroole ega pääsukoode teiste isikutega, isegi mitte oma lastega (kui toimepanijaks on nende isa, võivad lapsed paroole temaga jagada).

Ärge salvestage paroole ega pääsukoode arvutisse ega telefoni. Kui brauserid nagu Chrome, Edge jne küsivad teilt, kas soovite oma paroolid tulevikus kasutamiseks meelde jätta, siis keelduge sellest. Arvestage, et kui te juba kasutate kontodele sisselogimiseks salvestatud paroole, võib teie partneril olla neile juurdepääs. Paroole saab turvaliselt salvestada spetsiaalsetesse paroolihalduri rakendustesse.

Looge suhtluse haldamiseks **uus e-posti konto**. Kasutage seda e-posti kontot ka teiste kontode seadistamiseks (pank, tervishoiuteenused, kindlustus jne) ja juhuks, kui vajate oma isiku kinnitamiseks

teist e-posti aadressi. Võimaluse korral ärge kasutage e-posti aadressis oma ees- ega perekonnanime, vaid valige muu nimi (mitte TeieEesnimiPerekonnanimi@email.com).

Looge oma turvalise seadme jaoks uus Google'i või iCloudi konto. Pidage meeles, et Google'i või iCloudi kontod salvestavad sageli teavet nii teie kui ka teie elu kohta (näiteks fotosid, e-kirju, kontakte, faile jm). Seega on oluline, et valiksite oma uue konto kaitsmiseks tugeva parooli, mida te kellegagi ei jaga.

Desaktiveerige nutikodu seadmed, nagu Google Nest, Siri või Alexa, mida saab kasutada vestluste pealtkuulamiseks.

Kasutage navigeerimisel brauseris inkognito režiimi, et külastatud veebisaitidest ei jääks maha jälgi.

Logige tegevuse lõpetamisel veebilehtedelt ja kontodelt, eriti sotsiaalmeedia ja e-posti kontodelt välja. Kui sulgete lihtsalt brauseriakna, võib mõni teine arvutit kasutav inimene teie kontodele juurde pääseda.

Kontrollige sotsiaalmeedia privaatsussätteid ja seadistage need kõrgeimale privaatsustasemele. Tehke sama oma laste kontodega.

Olge ettevaatlik selle suhtes, mida te veebis postitate. Vältige postitusi, mis võivad paljastada teie asukohta, kahjustada teie mainet või mida võidakse teie vastu kasutada. Teadke, kes teie postitusi näevad, ja ärge unustage, et sõbrad ja jälgijad saavad teha teie piltidest ja postitustest kuvatõmmiseid ning neid teistega jagada. Üldreeglina:

- ⇒ ärge jagage isiklikku teavet (nimi, aadress, sünnikuupäev, telefoninumber);
- ⇒ ärge märkige piltide juurde oma asukohta;
- ⇒ paluge sugulasi ja sõpru, et nad ei postitaks pilte teist ega teie lastest ega märgiks teid ega teie lapsi oma piltidel.

Valige, keda te sotsiaalmeedias oma sõprade ja jälgijatena lisate. Lisage ainult inimesi, kelle puhul saate kindel olla, et nad ei suhtle toimepanijaga.

Kontrollnimekiri ohvritega töötavatele spetsialistidele

Kübervägivalla ja elektrooniliste seadmete puhul on olemas mõned ohumärgid, mis võivad ohvrile ja teda toetavale spetsialistile anda märku jälitustarkvarast või muudest kübervägivalla vormidest.

Ohver ei pruugi sageli kübervägivalla vorme ega ulatust teada. Oluline on olla aktiivne ja kontrollida kübervägivalla võimalikkust isegi siis, kui teie poole pöördunud naine ei väljenda selle suhtes mingit muret ega kahtlust. Naine ei pruugi olla toimuvast teadlik või ta ei pea seda probleemiks.

Alljärgnevat töövahendit ei tohiks käsitleda ohvrile esitatavate küsimuste loeteluna, vaid pigem kogumina ohumärkidest, mis võib viidata jälitustarkvara olemasolule või muudele digivahendite kaudu toimepandavatele kontrollivormidele. Oluline on meeles pidada, et kübervägivald ei piirdu ainult küberjälitamisega, vaid hõlmab ka muid vägivalla vorme, nagu küberahistamine, loata piltide jagamine (kuni seksuaalse väljapressimise (*sextortion*) ja kättemaksupornoni), inimkaubandus jne.

Töövahendis on esitatud ohumärgid, mis on jagatud nelja rühma:

- nutitelefonide (või muude seadmete) tehnilised aspektid,
- seadmete ja kontode kasutamine,
- toimepanija käitumine,
- sotsiaalmeedia.

Iga ohumärgi puhul on loetletud sellega seotud ohud, võimalik kübervägivalla vorm ja nõuanded tegutsemiseks.

PIDAGE MEELES: enne mis tahes allpool loetletud vastumeetme rakendamist on esmatähtis luua koos naisega selge ja põhjalik **IT-turvalisuse plaan** (vt täpsemalt eespool). Pidage alati meeles, et järsud muudatused võivad toimepanija vägivaldset käitumist eskaleerida.

Nutitelefoni või muude seadmetega seotud tehnilised ohumärgid

OHUMÄRK	Jah	Ei	Oht	Kübevägivalla vorm	Mida teha, kui vastus on „jah“?
Mobiilseade kadus mõneks ajaks ja ilmus siis uuesti välja			Need märgid viitavad sellele, et seadmesse võib olla paigaldatud jälitustarkvara rakendus	Küberjälitamine, jälitustarkvara	Kontrollige, kas toimepanija on paigaldanud seadmesse jälitustarkvara rakenduse. Kui jälitustarkvara olemasolu on kinnitust leidnud, planeerige hoolikalt järgmisi samme. Pidage meeles kõiki jälitustarkvara haldamisega seotud turvalisuse küsimusi
Mobiiltelefoni/tahvelarvutit/lauaarvutit/nutikella kasutab ka partner					
Telefoni aku tühjeneb varasemast kiiremini					
Rakenduste loendisse on tekkinud uus rakenduse ikoon, mida ohver ei tunne					
Telefoni mobiilse andmeside kasutus on suurenenud					
Toimepanija kinkis ohvrile või tema lastele uued seadmed			Need rakendused võimaldavad paigaldada telefonidesse tarkvarapakette	Häkkimine, küberjälitamine, loata piltide jagamine	Kustutage vanadest seadmetest kõik andmed
Telefonis on rakendus nimega Superuser (Android) või Cydia (iOS)					
Mõnel rakendusel on asukoha ja/või kaamera õigused isegi siis, kui neid ei ole konkreetsele rakendusele algselt antud			Seadmesse võib olla paigaldatud rakendusi, mis jagavad asukohateavet või kasutavad kaamerat, ilma et naine sellest teadlik oleks		Kontrollige regulaarselt, kas load on tühistatud
Ohver vahetas hiljuti oma mobiiltelefoni ilma vanast telefonist andmeid kustutamata			Toimepanijal võib olla juurdepääs vanale telefonile ning seal salvestatud andmetele ja rakenduste kontodele (e-post, sotsiaalmeedia jne)		

Seadmete ja kontode kasutamisega seotud ohumärgid

OHUMÄRK	Jah	Ei	Oht	Kübertõlvivalla vorm	Mida teha, kui vastus on „jah“?
Seadmetel puudub avamiskaitse või seadme/konto parool on lihtne ja erinevatel kontodel sama			Toimepanijal võib olla seadmele või erinevatele veebikontodele juurdepääs	Küberjälitamine, loata piltide jagamine	Muutke paroole regulaarselt ja valige keerulised paroolid
Paroolid on salvestatud arvutis/seadmes, millele toimepanijal on juurdepääs					Vahetage ekraani avamise meetod PIN-koodi või mustritu vastu. Pidage silmas, et ka PIN-kood ei ole alati turvaline, kuna see on hõlpsasti nähtav
Ohver kasutab seadme avamiseks sõrmejälge või näotuvastust			Toimepanija võib olla suuteline seadme lukust lahti tegema, kui ohver magab		Katkestage ja tühistage juurdepääs sõnumirakendustele (seda saab teha mobiiltelefonist). Vältige nende rakenduste kasutamist jagatud seadmetes
Sõnumirakendused (nagu WhatsApp Web, Messenger, Viber vms) on paigaldatud arvutitesse või tahvelarvutitesse, millele pääsevad juurde ka teised inimesed			Toimepanijal võib olla võimalus lugeda ohvri vestlusi ning näha fotosid ja videoid		Muutke paroole
Partnerid on omavahel vahetanud sotsiaalmeediakanalite paroole/kontosid					
Seadet kasutavad ka paari lapsed			Toimepanija võib paluda lastel anda talle edasi ohvri telefonis olevate sõnumite sisu	Jälgimine, küberjälitamine	Muutke paroole ja takistage laste juurdepääsu oma ema kontodele
Partneril on juurdepääs naise pangaandmetele			Toimepanijal on võimalik kontrollida pangatehinguid ja lubada ülekandeid	Küberjälitamine, majanduslik vägivald	Muutke internetipanga sisselogimisandmeid
Naise autol on integreeritud GPS-süsteem			Toimepanija saab jälgida, kuhu ohver läheb ja mis teed kaudu ta sinna läheb	Jälitamine, küberjälitamine	Rääkige usaldusväärse mehaanikuga auto GPS-funktsiooni väljalülitamise võimalusest
Toimepanijal on juurdepääs ohvri Google'i kontole			Google'i konto kaudu saab toimepanija igal ajal jälgida ohvri telefoni asukohta ja kontrollida asukohtade ajalugu (Google Mapi ajajoon)		Lülitage telefonis välja asukoha ajalugu ja muutke parooli

Kodus on nutikodu seadmed (näiteks Alexa, Siri, Google Home, Google Nest jne)			Neid seadmeid saab häkkida, et vestlusi pealt kuulata	Jälgimine, küberjälitamine	Desaktiveerige seadmed või vähemalt arvestage nende olemasoluga
---	--	--	---	----------------------------	---

Partneri/toimepanija käitumisega seotud ohumärgid

OHUMÄRK	Jah	Ei	Oht	Kübertõrjumise vorm	Mida teha, kui vastus on „jah“?
Mõnikord teab toimepanija infokilde, mida temaga ei ole arutatud ega jagatud			Toimepanija võib jälgida ohvri telefoni või on tal juurdepääs ohvri sotsiaalmeediakontodele	Jälgimine, jälitustarkvara	Kontrollige, kas seadmes on jälitustarkvara
Toimepanijat on nähtud kohtades, kus naine tavaliselt ei käi, ilma et naine oleks talle oma käikudest rääkinud			Toimepanija võib jälitada naise telefoni või autot	Jälitamine, jälitustarkvara	Kontrollige, kas seadmes on jälitustarkvara. Rääkige usaldusväärse mehaanikuga auto GPS-funktsiooni väljalülitamise võimalusest ja võimalusel desaktiveerige auto GPS
Toimepanija tsiteerib katkeid sõnumitest/telefonivestlustest, mida naine on teiste inimestega vahetanud/pidanud			Toimepanija võib jälgida naise telefoni või tal on juurdepääs naise sõnumirakendustele või kontodele	Jälgimine, jälitustarkvara	Kontrollige, kas seadmes on jälitustarkvara, muutke kontode parooli
Naine on kindel, et mees ei jälita teda, kuid leiab, et tema partner teab liiga hästi, kus ta käib			Toimepanija võib jälgida ohvri telefoni	Jälitamine, jälitustarkvara	Kontrollige, kas seadmes on jälitustarkvara
Naise partner ei küsi enam tema telefoni näha ega nõua tema parooli			Toimepanija võib olla paigaldanud naise telefoni jälitustarkvara		
Mees tahab seksida samas ruumis ja samas kohas konkreetsetel tingimustel			Ruumis võivad olla peidetud salvestusseadmed	Loata piltide jagamine, <i>doxing</i> , <i>sexting</i> , kättemaksuporno, <i>sexortion</i>	Kontrollige, kas ruumis on salvestusseadmeid; võimalusel katke need riietega

Sotsiaalmeediaga seotud ohumärgid

OHUMÄRGID	Jah	Ei	Oht	Kübertvõimurite vorm	Mida teha, kui vastus on „jah“?
Naisega on sotsiaalmeedias ühendust võtnud võõrad inimesed			Toimepanija võib olla loonud ohvri jälgimiseks võltsprofiile; toimepanija võib olla veebis jaganud ohvri kontaktandmeid	Jälgimine, veebiahistamine, <i>sexting</i> , <i>doxing</i>	Kontrollige tundmatu profiili pilte, postitusi, jälgijaid ja ühiseid kontakte
Naine jagab sageli oma asukoha kohta fotosid ja üksikasju sotsiaalmeedias või WhatsAppi stoorides			Neid andmeid saab kasutada ohvri jälitamiseks ja jälgimiseks. WhatsAppi stoorisid saab vaadata isegi inimene, kes ei ole ohvri kontaktide hulgas	Jälgimine, küberjälitamine, loata piltide jagamine	Rääkige ohvriga sellest, kui oluline on hinnata, milline mõju tema postitustel võib olla
Naine on oma partneriga jaganud sotsiaalmeediakontode parooli			Partneril on juurdepääs naise kontodele, vestlustele, sõpradele/jälgijatele ja ta saab omandada pilte		Muutke parooli. Rääkige ohvriga sellest, kui oluline on parooli teistega mitte jagada, isegi hädaolukordades
E-posti aadress parooli taastamiseks on juurdepääsetav ka partnerile			Sellisel juhul saab toimepanija lihtsasti naise parooli muutmiseks teada. Toimepanija saab ka ise naise parooli muuta, muutes kontod naisele endale juurdepääsmatuks	Jälgimine, küberjälitamine, identiteedivargus	Muutke taasteaadressi enne paroolide muutmist
Naine on märganud oma sotsiaalmeediakontodel kahtlast tegevust, nagu oleks kellelgi olnud neile juurdepääs			Kellelgi, mitte tingimata partneril, võib olla naise kontodele juurdepääs	Küberjälitamine, identiteedivargus, loata piltide jagamine	Muutke parooli
Naine on saanud „kiidukõnesid“ ja/või -sõnumeid võõrastelt			Võimalik, et veebis on avaldatud naise kontaktandmeid ja intiimseid pilte temast	<i>Doxing</i> , <i>sexting</i> , loata piltide jagamine, küberahistamine, kättemaksuporno	Jälgige kõnesid/sõnumeid, seadistage Google Alerts, taotlege eemaldamist otsingumootoritest
Naisele helistatakse tema kontaktide numbritelt, kuid vastates selgub, et helistajaks on toimepanija			Toimepanija võib kasutada rakendusi, mis võltsivad tema helistaja ID-d	<i>Spoofing</i> , ahistamine	Hoidke nende kõnede logi koos telefonikõne andmetega alles



Abi ja nõu kübervägivalla esinemise või kahtluse korral:

- Kui ohus on elu ja tervis, helista **112**
- **116 006** – sotsiaalkindlustusameti ohvriabi kriisitelefoni, mis pakub kriisinõustamist ööpäevaringselt. Välismaalt helistades +372 614 7393.
- **116 111** – sotsiaalkindlustusameti lasteabitelefoni
- **660 6077** – sotsiaalkindlustusameti vägivallast loobumise tugiliini (tööpäeviti kell 10.00-16.00)
- **palunabi.ee** – sotsiaalkindlustusameti ohvriabi veebileht, kust saab nõu mh ka tekstivestluses
- **lasteabi.ee** – sotsiaalkindlustusameti lasteabi veebileht, kust saab nõu mh ka tekstivestluses
- **Vaimse tervise veebinõustamine** - sotsiaalkindlustusameti tasuta teenus, millele saab registreeruda iseteenindusest:
<https://www.sotsiaalkindlustusamet.ee/abivajav-laps-ja-taiskasvanu/vaimne-tervis-kriisis/vaimse-tervise-veebinouustamine>
- **Naiste tugikeskused** – tugikeskusest saad terviklikku abi kõigi naistevastasevägivalla vormide puhul, sh ka kübervägivalla
<https://www.sotsiaalkindlustusamet.ee/abivajav-laps-ja-taiskasvanu/abi-vagivalla-ohvrile/naiste-tugikeskused#naiste-tugikeskuste-kontaktid>
- **Veebipolitseinikud** - <https://www.politsei.ee/et/veebipolitseinikud> **Milliste muredega veebipolitseiniku poole pöörduda?**
 - Kui soovid politseilt nõu ja sul on seadusi puudutavaid küsimusi
 - Kui kahtlustad, et keegi teine esineb internetis sinu nime all
 - Kui oled sattunud kiusamise/ahistamise ohvriks
 - Kui soovid teatada seksuaalsest või muust väärkohtlemisest