DIGITAALINEN TURVA-SUUNNITELMA

Kuinka suojautua digitaaliselta väkivallalta?

Tämä turvasuunnitelma on tarkoitettu digitaalista väkivaltaa erityisesti lähisuhteessaan kokeville itsenäiseen tilanteen arviointiin ja turvaamiseen. Samalla se on työkalu ammattilaisille väkivaltaa kokevan asiakkaan digitaalisen turvallisuuden arviointiin yhdessä asiakkaan kanssa.

Tarkistuslista toimii erityisesti niissä tilanteissa, joissa epäillään tai on jo näyttöä teknologian välityksellä tapahtuneesta kontrolloinnista ja muusta digitaalisesta väkivallasta.

2025

Naisten Linja

Naisten Linja

Muistathan aina ensin

1. Varmistaa fyysinen turvallisuutesi! Asutko väkivallan tekijän kanssa, tai onko hänellä pääsy kotiisi? Joskus digitaalisen väkivallan rajaaminen voi eskaloida väkivaltaa.

2. Dokumentoida välittömästi kaikki epäilyttävät löydökset ottamalla niistä valokuvat, kuvakaappaukset, videotallenne tai varmuuskopiot. Ne voivat toimia todistusaineistona mahdollisessa rikosprosessissa.

1. Suojaa tilisi ja laitteesi

- [ ] Vaihda salasanat kaikille tileillesi. Käytä pitkiä ja monimutkaisia salalauseita, jotka on mahdotonta arvata (älä käytä esim. omia merkkipäiviä tai läheisten nimiä). Vähintään 15 merkkiä pitkä salasana suojaa tehokkaasti.
    - [ ] Jos epäilet, että laitteessasi on vakoiluohjelma, käytä salasanojen vaihtoon turvallista laitetta (ystävän puhelin, kirjaston tietokone). Älä tallenna uusia salasanoja esim. Google-tilillesi.
- [ ] Ota käyttöön monivaiheinen tunnistautuminen kaikissa palveluissa, joissa se on mahdollista.
- [ ] Käytä laitteissasi sim-kortin ja näytön lukitusta. Vältä sormenjälkitunnistusta, mikäli on mahdollista, että joku pystyy avaamaan sen sormellasi esimerkiksi nukkuessasi.
- [ ] Ota sovelluksissa ja palveluissa käyttöön kirjautumisilmoitukset, jolloin saat esim. sähköpostiin ilmoituksen, kun tilillesi kirjaudutaan uudelta laitteelta.
- [ ] Pidä sovellusten, käyttöjärjestelmien, älylaitteiden (esim. älykellot, -TV:t ja verkkoon liitetyt kodinkoneet ja valvontakamerat) ja WiFi-modeemin päivitykset ajan tasalla. Käytä myös niiden suojaamiseen vahvoja salasanoja, ja vaihda aina oletussalasanat!
- [ ] Vältä avoimien WiFi-verkkojen käyttöä, koska niissä ulkopuolisen on helpompi päästä käsiksi tietoihisi. Käytä esim. puhelimesi mobiiliverkkoa. VPN-palvelu tuo lisäturvaa.

2. Jos nykyinen kumppanisi kontrolloi tekemisiäsi

- [ ] Jos epäilet, että puhelintasi käytetään vakoiluun, käy eroaikeisiin ja muihin arkaluontoisiin asioihin liittyvät keskustelut muulla laitteella kuin omillasi (esim. salainen prepaid-puhelin, kirjaston kone) tai kasvotusten.
    - [ ] Älä pidä puhelinta mukana arkaluontoisissa keskustelutilanteissa.

- [ ] Tee uusi salainen sähköposti arkaluontoisia sähköposteja varten, ja käytä sitä vain turvallisella laitteella.

- [ ] Vältä Bluetooth-laitteiden käyttöä, kun puhut puheluita. Laitteisiin (esim. kuulokkeet) on mahdollista murtautua salakuuntelemaan bluetooth-yhteyden kautta.

- [ ] Käytä nettiä ”yksityinen selaus” tai “incognito”-tilassa. Poista sivuhistoriasta riskialttiit sivut. Vieraile riskialttiilla sivuilla ensisijaisesti muilla kuin omilla laitteillasi. Huomioi, että tekijä voi osata palauttaa myös tietokoneelta hiljattain poistetut tiedot.

- [ ] Ota pikaviestipalveluissa “luettu”-kuittaukset ja “viimeksi paikalla” -tieto pois päältä.

3. Jos epäilet, että sinua seurataan laitteiden kautta

- [ ] Varmista, ettei puhelimesi tai käyttämäsi sovellukset jaa tai tallenna sijaintitietoja. Laita sijainnin seuranta pois päältä Google- tai AppleID-tililläsi.

- [ ] Laita Bluetooth pois päältä, kun et käytä sitä.

- [ ] Tarkista Google- tai AppleID-tilisi sekä käyttämiesi somepalveluiden asetuksista sisäänkirjautuneet laitteet (esim. nimillä “linkitetyt laitteet”, “aktiiviset istunnot” tai “kirjautumishistoria”), ja kirjaa ulos kaikki sinulle tuntemattomat laitteet.

- [ ] Tarkista sähköpostin edelleenlähetysasetus sekä eri sovellusten varmuuskopiointi-asetukset (esim. kuvien tai viestien varmuuskopiointi).

- [ ] Käy läpi laitteessasi olevat sovellukset laitteen asetuksista. Onko jotain mitä et tunnista? Ota selvää, mistä sovelluksesta on kyse.

    - [ ] Kiinnitä erityistä huomiota sovelluksiin, jotka liittyvät varmuuskopiointiin tai “parental control” tai “family link” -tyyppisiin palveluihin. Käy läpi myös viattomalta vaikuttavat sovellukset, kuten “asetukset” ja “WiFi”; jos tällaiset sovellukset pystyy poistamaan laitteesta, voi kyseessä olla haitallinen sovellus.

- [ ] Hanki uudet laitteet tai palauta tehdasasetukset/uudelleenasenna käyttöjärjestelmä vanhoissa laitteissasi. Tehdasasetusten palautus poistaa seurantaohjelmat suurimmassa osassa tapauksista (huomioi, että myös mahdollinen todistusaineisto katoaa!).

    - [ ] Älä käytä toimintoa, jossa puhelimeen asennetut sovellukset kopioidaan pilvipalveluun ja asennetaan suoraan uudelle tai puhdistetulle puhelimelle. Lataa tarvitsemasi sovellukset manuaalisesti sovelluskaupasta.

Naisten Linja

4. Jos pelkäät tietojesi tai kuviesi leviävän verkossa

- [ ] Jos väkivallan tekijä uhkaa levittää sinusta intiimejä kuvia tai videoita verkossa, voit käyttää StopNCII-palvelua kuvien jäljittämiseen (jos sinulla on kyseinen kuvamateriaali hallussasi).
- [ ] Muunlaisia kuvia voi etsiä Googlen käänteisellä kuvahaulla (huomioi Googlen tietosuojakäytännöt ja oma yksityisyytesi).
- [ ] Henkilötietojen leviämistä voi seurata Googlen Alerts-toiminnolla, joka toimii hakuvahdin tavoin. Käytä etsittävinä sanoina esim. nimeäsi, osoitettasi, nimimerkkiäsi, puhelinnumeroasi yms.

5. Suojaa yksityisyytesi ja henkilötietosi

- [ ] Käy sovellusten ja käyttäjätilien tietoturva- ja yksityisyysasetukset läpi, ja suosi mahdollisimman vahvaa yksityisyyttä (esim. sijaintitiedot, profiilin näkyvyys, kuka voi lähettää viestejä).
- [ ] Mikäli väkivallantekijällä on ollut pääsy verkkopankkitunnuksiisi, ole yhteydessä pankkiin tunnusten vaihtamiseksi.
- [ ] Harkitse tarpeen mukaan erilaisia tiedonluovutuskieltoja:
    - [ ] Numeron salaaminen operaattorin kautta
    - [ ] Yhteystietojen luovutuskielto Digi- ja väestötietovirastossa
    - [ ] Auton omistajalle: tietojen salaaminen Traficomissa
    - [ ] Verohallinnon Positiivisen luottotietorekisterin kautta voit tehdä vapaaehtoisen luottokiellon ja tarkastella nimissäsi olevia luottoja
    - [ ] Turvakielto Digi- ja väestötietovirastossa on järeämpi suojaus, joka vaatii erityisperusteet

Tarvitsetko tukea tai neuvontaa digitaaliseen väkivaltaan liittyen? Naisten Linja tarjoaa maksutonta ja luottamuksellista keskusteluapua ja tukea digitaalista väkivaltaa kokeneille naisille ja tytöille.