

Ohjeita politiikassa toimiville henkilöille

Verkkohäirinnän riskien
ennakointi ja hallinta

SUVI VEPSÄ

IDA

intimiys datavetoisessa kulttuurissa



TURUN YLIOPISTO 2021

ISBN 978-951-29-8407-7

Sisällys

1.1. Yleisimmät verkkohäirinnän taktiikat	4
1.2. Häirintätilanteissa toimiminen ja häirinnän riskien minimointi	6
1.3. Lisätietoa verkkohäirinnästä ja tietoturvallisuudesta	9

Ohjeita politiikassa toimiville henkilöille

1.1. Yleisimmät verkkohäirinnän taktikat

Verkkohäirintä: Verkkohäirinnällä tarkoitetaan kommenttien, kuvien tai videoiden muodossa esiintyvää häiritsevää ja loukkaavaa toimintaa, jonka tarkoituksena on loukata, nöyryyttää tai vaientaa häirinnän kohde. Verkkohäirinnän muotoja ovat esimerkiksi vihapuhe, häiritsevä viestittely, seksuaalinen häirintä, uhkailu ja pelottelu.

Verkkoviha: Verkkoviha on eräänlainen kattotermi monille vihapuheen ja häirinnän eri muodoille. Laajan määritelmän mukaan verkkovihaa on esimerkiksi häiritsevän materiaalin levittäminen, rasismi, antisemitismi, uskonnollinen kiihkoilu, homofobia, vammaisiin kohdistuva vihamielisyys, poliittinen viha, naisviha, suostumukseton pornografia, terrorismin edistäminen, nettikiusaaminen, huhujen levittäminen, ahdistelu ja vainoaminen, vastapuheen vaientamiseen pyrkivä puhe sekä eri ryhmiä leimaava puhe.

Vihapuhe: Vihapuhe määritellään sellaiseksi henkilöön tai henkilöryhmään kohdistuvaksi puheeksi, jolla levitetään, yllytetään tai edistetään vihaa, joka perustuu henkilön ihonväriin, syntyperään, kansalliseen tai etniseen alkuperään, ikään, vammaisuuteen, kieleen, uskontoon tai vakaumukseen, sukupuoleen, seksuaalisuuteen tai muuhun henkilökohtaiseen ominaisuuteen tai asemaan. Vihapuhe on viestintää, jonka tarkoitus on sulkea jokin ryhmä ulkopuolelle tai luoda ryhmään kuuluvista ihmisistä kuva epäilyttävänä, epäluotettavana tai alempiarvoisina. Suomessa vihapuheelle ei ole lainopillista määritelmää, eikä lainsäädännössä ole määritelty rikosta, jonka rikosnimike olisi vihapuhe. Vihapuhe on kuitenkin rikos silloin, kun se täyttää jonkin rikoksen tunnusmerkistön. Tällaisia rikoksia ovat esimerkiksi kiihottaminen kansanryhmää vastaan sekä uskontorauhan rikkominen. Vihapuhe ei

ole aina näkyvästi vihaista tai aggressiivista, vaan myös rauhalliseen sävyyn argumentoitu puhe voi olla vihamielistä tai vihaa lietsovaa. Merkitystä on sillä, mitä sanotaan.

Doksaus: Doksauksella tarkoitetaan toisen henkilökohtaisten, usein arkaluontoisten tietojen etsimistä, keräämistä, anastamista ja levittämistä verkkoon.

Hakkerointi: Hakkeroinnilla tarkoitetaan teknologian hyödyntämistä henkilön yksityisten tietojen sieppaamiseen, tietojen muokkaamiseen tai uhrin mustamaalaamiseen. Esimerkiksi murtautuminen tietokantoihin, sivustoihin, yksityisiin tileihin tai laitteisiin sekä virusten tai vakoiluohjelmien asentaminen.

”Kostoporno” ja seksuaalinen häirintä: Seksuaalinen häirintä verkossa voi olla esimerkiksi seksuaalisten kuvien ja viestien lähettämistä ja jakamista ilman vastaanottavan tahon suostumusta tai seksuaalissävytteistä uhkailua. Niin kutsuttu kostoporno tai suostumukseton pornografia tarkoittaa aiemmin yhteisymmärryksessä ja luottamuksessa jaettujen, varastettujen tai salaa otettujen intiimien kuvien tai videoiden luvaton levittämistä verkkoon. Tarkoituksena on uhrin nöyryyttäminen ja tämän maineen pilaaminen. Kostopornoon voi liittyä myös kiristystä ja uhkailua.

Maalittaminen ja laumahyökkäykset: Maalittaminen tarkoittaa verkossa, useimmiten sosiaalisessa mediassa tapahtuvaa ”maalitauluksi ottamista”, eli ihmisten usuttamista tietyn henkilön kimppuun. Maalittamisen seurauksena henkilöön voi kohdistua laumahyökkäyksiä, suuria määriä vihamielisiä viestejä ja häirintää, joiden taustalla voi olla satoja ihmisiä. Pyrkimyksenä on vaientaa uhri ja esimerkiksi viedä tältä mahdollisuudet työhön. Maalittamiseen voikin liittyä myös yhteydenottoja kohteen työnantajaan tai yhteistyökumppaneihin.

Trollaus: Trollauksen määritelmä on laaja: sillä voidaan tarkoittaa kaikkea vakavammasta vihapuheesta leikkimielisempään meemien ja viestien levittämiseen. Yleisimmin trollaus käsitetään toistuvana häiritsevien, loukkaavien tai muuten kyseenalaisten viestien levittämisenä sosiaalisessa mediassa ja erilaisilla keskustelupalstoilla tavoitteena provosoida ja aiheuttaa reaktiota. Trollaus voi olla myös järjestelmällisempää, ammattimaisesti tuotettua ja jotakin poliittista ideologiaa palvelevaa.

Valetilit ja verkkoimitointi: Verkkoimitoinnilla tarkoitetaan toisen ihmisen esittämistä verkkoalustoilla. Kohteesta saatetaan esimerkiksi luoda valetilejä sosiaaliseen mediaan ja sitä kautta julkaista lausuntoja ja mielipiteitä, jotka tuottavat haittaa häirinnän kohteelle ja tämän maineelle. Toisena esiintyminen voi myös olla tapa kalastella yksityisiä ja arkaluonteisia tietoja.

Verkkokiusaaminen: Verkkokiusaaminen on verkossa tapahtuvaa toistuvaa ja tarkoituksellista häirintää, jonka tavoitteena on uhrin loukkaaminen, nöyryyttäminen tai pelottelu. Tällaista toimintaa on esimerkiksi toistuvat loukkaavat kommentit, huhujen levittäminen ja uhkailu.

Verkkovainoaminen: Verkkovainoaminen tarkoittaa henkilön systemaattista häirintää ja vainoamista esimerkiksi sosiaalisessa median, viestisovellusten tai sähköpostin kautta. Verkkovainoamisella tarkoitetaan myös verkon ja teknologian hyödyntämistä henkilön vakoiluun, seurantaan tai yksityisten tietojen keräämiseen.

1.2. Häirintätilanteissa toimiminen ja häirinnän riskien minimointi

Pyri ennakoimaan häirintätilanteet

Politiikassa toimiviin henkilöihin kohdistuva häirintä on hyvin yleistä. Häiritseviin tai uhkaaviin tilanteisiin on hyvä varautua jo ennalta. Häirintään kannattaa varautua erityisesti vaalien alla ja silloin, kun päätöksiä tehdään erityisen paljon tunteita herättävistä aiheista.

Selvitä, onko puolueessasi valmiina toimintasuunnitelmaa tai -ohjeistusta häiritseviin tilanteisiin. Kehen voit tarvittaessa olla yhteydessä ja mistä hakea apua?

Tunnista tilanne

Häirintätilanteissa on hyvä määritellä, millaisesta häirinnästä on kyse, jotta tilanteisiin voitaisiin reagoida parhaalla mahdollisella tavalla. Onko kyseessä joukkoistettu vihakampanja vai yksittäinen häirikkö? Vaarantaako häirintä yksityisyytesi tai turvallisuutesi? Kohdistuuko häiritsevä palaute työhösi vai sinuun henkilönä? Tutustu yleisimpiin verkkohäirinnän taktiikoihin.

Älä jää yksin

Häirinnän ja vihapuheen kohteeksi joutuminen voi olla erittäin raskasta. On tärkeää muistaa pyytää tukea, jos koet siihen tarvetta. Häirinnästä on joka tapauksessa hyvä ilmoittaa jollekin luotettavalle henkilölle.

Tukea voi saada myös oman piirin toiminnanjohtajalta, puolueen häirintäyhdyshenkilöltä, kunnalta, eduskunnan turvallisuusosastosta tai eduskuntaryhmästä, tilanteestasi riippuen. Muista myös vertaistuen mahdollisuus.

Ota viestit talteen

Tallenna kaikki mahdolliset tapahtumaan liittyvät todisteet. Ota viipymättä näyttökuva kaikista vihapuhetta ja häirintää sisältävästä sisällöstä. Säilytä sähköpostit ja yksityisviestit. Kirjaa ylös myös mahdolliset häiritsevät puhelut. Todistusaineistosta on hyötyä, mikäli joudut tekemään häirinnästä rikosilmoituksen. Tallenna viestit mieluiten niin, että mukana on aikaleima ja tiedot viestin lähittäjästä.

Jos viestien tallentaminen tuntuu liian raskaalta, pyydä jotakuta läheistäsi tai kollegaasi auttamaan.

Ilmianna ja estä kirjoittaja.

Sinulla ei ole velvollisuutta kommunikoida häiritsevien ihmisten kanssa. Sosiaalisen median alustat tarjoavat mahdollisuuden ilmiantaa häiritsevästi käyttäytyvät profiilit. Kun olet ottanut häiritsevät viestit talteen, vaadi sivuston ylläpitäjältä niiden poistamista.

Ilmiantamisen lisäksi häiritsevät tilit kannattaa estää. Estämisen jälkeen häirikkö ei voi enää nähdä profiiliasi tai viestejäsi.

Mieti, kannattaako viesteihin vastata

Viesteihin vastaaminen voi olla hyvä keino vastustaa häirintää. Vastaamista kannattaa kuitenkin punnita tarkkaan, sillä joskus vastaaminen aiheuttaa lisää häiriköintiä. Et ole velvollinen vastaamaan kaikkiin saamiisi viesteihin.

Häirinnän ja vihapuheen tarkoituksena on usein hiljentää ei-toivotut mielipiteet ja vaikuttaa poliittiseen päätöksentekoon. Häirintätilanteissa keskity ensisijaisesti työhösi sekä omaan hyvinvointiisi.

Huolehdi turvallisuudestasi

Omasta tietoturvasta huolehtiminen on tärkeä muistaa.

Varmista, että salasanasi ovat tarpeeksi vahvoja. Älä käytä samaa salasanaa useissa eri palveluissa. Uhkaavissa tilanteissa vaihda salasanat välittömästi.

Kaksivaiheisen tunnistautumisen käyttöönotto eri palveluissa ja sovelluksissa on tehokas tapa ehkäistä tileillesi murtautuminen.

Sulje sijainnin jako sekä älypuhelimestasi että tietokoneestasi. Myös jotkut sosiaalisen median alustat saattavat jakaa sijaintiasi automaattisesti julkaisujesi kautta, joten tämä kannattaa tarkistaa.

Pidä huoli, ettei kukaan pääse käsiksi yksityiseen tietokoneeseesi tai muihin elektroniisiin välineisiin. Lukitse laitteesi ja ole huolellinen siinä, kenelle annat niihin pääsyn.

Jos epäilet, että puhelimessasi on vakoiluohjelma, älä yritä poistaa sitä itse, vaan toimita laite poliisille tutkittavaksi.

Tarkista, kenellä on pääsy yhteystietoihisi

Onko esimerkiksi henkilökohtainen puhelinnumerosi tai osoitteesi yleisesti saatavilla? Harkitse, miten ja missä jaat yhteystietojasi. Joissain tilanteissa yhteystietojen saatavuutta voi joutua rajoittamaan.

Maistraatin kautta voi tarvittaessa tehdä myös tietojenluovutuskiellon tai turvakiellon.

Tarkista, mitä tietoja sinusta löytyy verkosta

Tarkista sometiliesi yksityisasetukset. Googlaa nimesi ja pyydä tarvittaessa tietojesi poistoa julkisilta sivustoilta ja rekistereistä.

Google Alerts -palvelun kautta voit saada ilmoituksen aina, kun esimerkiksi nimesi, osoitteesi, puhelinnumerosi tai muu haluamasi tieto mainitaan verkossa.

Mieti, mitä jaat sosiaalisessa mediassa ja kenelle

Mieti, mitä sosiaalisen median alustoja käytät mihinkin tarkoitukseen. Henkilökohtaiset sosiaalisen median tilit kannattaa suojata niin, etteivät tuntemattomat pääse näkemään tietojasi ja päivityksiäsi. Työkäyttöön ja muuhun julkiseen kommunikointiin kannattaa tehdä erillinen profiili tai sivu, johon ei jaeta henkilökohtaisia tietoja.

Tee tarvittaessa rikosilmoitus

Jos epäilet tilanteeseen liittyvän rikosta tai sen uhkaa, ole yhteydessä poliisiin.

Muista huolehtia henkisestä hyvinvoinnistasi ja jaksamisestasi

Jos tilanne on liian kuormittava, ota etäisyyttä. Tee asioita, joista nautit. Hae tarvittaessa apua. Muista, ettei häirintä ole koskaan sinun syysi.

1.3. Lisätietoa verkkohäirinnästä ja tietoturvallisuudesta

[Crash Override: Resource Center](#)

[Data Detox Kit](#)

[Do-It-Yourself Online Safety](#)

[Gender and Tech Resources: Zen and the art of making tech work for you](#)

[Hack Blossom: A DIY Guide to Feminist Cybersecurity](#)

[HeartMob](#)

[Mitigating Internet Trollstorms](#)

[Security in a Box: Digital Security Tools and Tactics](#)

[Speak Up & Stay Safe\(r\): A Guide to Protecting Yourself From Online Harassment](#)

[Tactical Tech: Activism on Social Media: A Curated Guide](#)

[The Rory Peck Trust: Digital Security](#)

[Women's Media Center: Online Abuse 101](#)