

Doxcare

**Doxxauksen
ja poliittisen häirinnän ennaltaehkäisy
ja vahingon minimointi**



Doxcare: Doxxauksen ja poliittisen häirinnän ennaltaehkäisy ja vahingon minimointi

Original text in English

Doxcare: Prevention and Aftercare for Those Targeted by Doxxing and Political Harassment

2020

crimethinc.com/2020/08/26/doxcare-prevention-and-aftercare-for-those-targeted-by-doxxing-and-political-harassment

Finnish translation

fi.crimethinc.com/2020/08/26/doxcare-doxxauksen-ja-poliittisen-hairinnan-ennaltaehkaisy-ja-vahingon-minimointi

Layout

No Trace Project

notrace.how/resources/#doxcare

Tässä oppaassa kerrotaan vaihe vaiheelta, kuinka suojautua verkkohäiritsijöiltä, miksi se on tärkeää, ja mitä tehdä, jos joudut ”doxxauksen” kohteeksi. Doxxaus tarkoittaa henkilökohtaisten tietojesi julkaisemista. On korkea aika ryhtyä toimiin yksityisyytesi turvaamiseksi, ja sitä varten tämä opas on kirjoitettu.

Contents

Johdanto: erään henkilön tarina	4
Mitä doxxaus tarkoittaa?	4
Ennaltaehkäisy on tehokkain hoito	5
Erillisten elämän osa-alueiden ylläpitäminen	6
Taktiikat	8
Poista itsesi tiedonvälittäjien kirjoista	8
Poista vanhat tilit	9
Vaihda käyttäjänimiä, sähköpostiosoitteita ja salasanoja	9
Suodata saatavilla olevaa tietoa ja muuta tietosuoja-asetuksiasi .	10
Jos sinut on doxxattu	11
Pitäisikö minun kertoa tästä julkisesti?	12
Heti kun olet tullut doxxatuksi	13
Uhkien arviointi	14
Ratkaisuja	16
Kun keskustelet työpaikalla ja perheen kanssa	16
Elämä jatkuu	18

Johdanto: erään henkilön tarina

”Olen ollut aktiivinen yhteisössäni jo monta vuotta. Siitä ei ole paljon aikaa, kun äärioikeistolaiset trollit löysivät ystäväni, perheeni ja työpaikkani some-tilit. Näin stalkkaaminen alkoi. Antirasistisen toimintani vuoksi he etsivät minusta valokuvia ja käyttivät keräämiään tietoja uhatakseni minua, perhettäni ja ystäväni.

Jokaisessa ahdistelevassa sähköpostissa ja somekommentissa he leimaavat 'terroristiryhmiksi' poliittiset projektit joihin osallistun, kuvailevat minua 'johtajaksi' ja kuvitteellisen 'väkivaltaisten vasemmistolaisten varjojoukon' jäseneksi, johon he haluavat puuttua 'vakavilla keinoilla'. Olivatpa nämä johtopäätökset vain surkeaa tutkimustyötä tai tarkoituksellisesti vääristeltyjä väitteitä, tällaisen toiminnan tulisi olla huolestuttavaa kaikille, joiden mielestä sortoa on vastustava.

Poistin sosiaalisen mediani heti kun sain tietää mitä oli meneillään—en yhtään häpeä, että minut yhdistetään taisteluun vapaamman maailman puolesta, mutta halusin suojella ystäväni ja sosiaalisia verkostojani. Jokainen, joka tuntee minut, tietää, että vastustan kaikenlaista kiihkoilua ja sortoa. Tästä en ole koskaan vaiennut. Trollit eivät käyneet kimppuuni mistään tietystä, yksittäisestä teosta johtuen, vaan he vastustavat kaikkea antirasistista, feminististä ja queer-aktivistista toimintaa. He pyrkivät eristämään ja pelottelemaan meidät hiljaisiksi yksi kerrallaan. Siksi meidän on seisottava toistemme rinnalla.

Haluan sinun tietävän tämän siltä varalta, että joudut joskus samaan tilanteeseen. Et ole yksin. Toivon, että tämä kirjoitus rohkaisee sinua pohtimaan niin omaa kuin läheistesi verkkoturvallisuutta huolellisemmin.

Robert Bowers, Pittsburghin synagoga-ampuja, keskusteli julkisesti antirasisteja doxxaavien alt-right-trollien kanssa. Minua vastaan käyty vainoamiskampanja osoittaa, että he ovat valmiita vaikka valehtelemaan ongelmia aiheuttaakseen. Ainoa tapa suojella itseämme on osoittaa tukea toisillemme jatkuvasti. Emme saa antaa heidän pelotella meitä.”

Mitä doxxaus tarkoittaa?

Doxxaus tarkoittaa henkilön yksityisten tietojen julkaisemista, tarkoituksena paljastaa henkilö ja pelotella häntä. Tämä voi aiheuttaa fyysistä, emotionaalista ja taloudellista vahinkoa doxxauksen kohteeksi joutuneelle. Sen tavoitteena on saada kohde luopumaan toiminnastaan sekä häpeämään

ideoitaan ja arvojaan. On tärkeää huolehtia verkkoturvallisuudestaan ennen doxxauksen kohteeksi joutumista—tai pikemminkin ennen kuin sinulla on edes syytä pelätä sitä. Usein doxxaaja odottaa julkaisemishetkeä, kunnes hän on kerännyt tarpeeksi tietoa. On mahdollista, että sinua stalkataan jo, etkä saa tietää siitä ennen kuin on liian myöhäistä.

Oletpa sitten tunnettu julkinen aktivisti tai vain satunnaisesti kuvioissa mukana, tulee sinun suojata sosiaalisia verkostojasi ja muita elämäsi kuuluvia piirejä—vaikka et uskoisikaan tekeväsi mitään huomiota herättävää. Hyvien tietoturvakäytäntöjen noudattaminen suojaa ystäviäsi, perhettäsi ja yhteisöäsi. Ihmisiä saatetaan liittää oikeistolaisten salaliittoteorioihin ”Antifan jäsenistä” vain siksi, että he kuuluvat sukupuoli- tai seksuaalivähemmistöihin, ”näyttävät vasemmistolaisilta”, soittavat bändeissä, osallistuvat tapahtumiin tai viettävät aikaa radikaaleissa tiloissa. Tietojen ei tarvitse olla oikeita tai perusteltuja, että voit joutua häirinnän kohteeksi. Häiritsijä tarvitsee vain yhden tiedon etsiäkseen lisätietoja verkosta.

Tietoisuus verkkoon jättämistäsi tiedoista voi suojata sinua viranomaisilta ja stalkkereilta. Koska valtion hallitsema valvonta on entistä kehittyneempää ja live-striimaus on yleistynyt mielenosoituksissa, pelkkä maskin käyttö ei välttämättä riitä. Kesäkuussa 2020 Philadelphiassa poliisi onnistui tunnistamaan naisen pelkän epätarkan kuvan perusteella. He seurasivat verkkoon jääneitä jälkiä kuin nauhaan pujotettuja helmiä, mukaan lukien Etsy-ostos, Twitter-tilit ja naisen ammattityösivu. Tulli ja rajavartiolaitos ovat alkaneet seuraamaan julkista sosiaalista mediaa. Verkkonäkyvyydestä huolehtiminen voi tehdä olosi turvallisemmaksi myös verkon ulkopuolella.

Ennaltaehkäisy on tehokkain hoito

Nyt on paras aika aloittaa. Doxxauksen jälkeen et välttämättä pysty enää poistamaan levitettyjä tietoja vaikka kuinka yrittäisit.

Lähestymistapoja on monia. Paras tapa varmistaa, ettei kukaan löydä sinusta mitään tietoja on tietysti se, ettei kerta kaikkiaan ole mitään löydettävää—jotkut ihmiset eivät kuitenkaan pysty poistamaan läsnäoloaan verkosta joko työn, perheen tai muiden velvollisuuksien vuoksi. On myös monia hyviä syitä ylläpitää online-persoonaa. On esimerkiksi ammattialoja, joissa työnantaja suorastaan odottaa että sinulla on sosiaalisen median

presenssi, tai pitää sen puutetta epäilyttävänä. Sosiaalinen media voi myös olla välttämätön yhteydenpidon väline. Onneksi on olemassa tapoja pitää ainakin osa elämästäsi turvassa palomuurin takana. Voit tarvittaessa karsia tietoja julkisista profileistasi ja ottaa käyttöön toimintatapoja, jotka rohkaisevat sinua ja ystäviäsi jatkamaan poliittista toimintaa. Tämä prosessi voi olla työläs. Se vie aikaa ja energiaa. Suosittelen tekemään sen ystävien, kämppäkavereiden tai perheenjäsenten kanssa. Yhdessä tekeminen auttaa vaikeiden ja tylsien vaiheiden läpi.

Erillisten elämän osa-alueiden ylläpitäminen

Jos et pysty täysin poistamaan itseäsi internetistä, voit silti säilyttää suhteellisen yksityisyyden ylläpitämällä erillisiä verkkotoiminnan osa-alueita ja siivoamalla tietoja pois harvoin käytetiltä tai unohdetuilta tileiltä.

Läsnäolosi verkossa on luultavasti monimuotoinen. Sosiaaliset verkostot, ilmoitustaulut, työ sivustot, sähköpostitilit—kaikki mihin on kirjaututtava sisään. Tyypillisesti doxxauksessa haravoidaan informaatiota useista eri lähteistä. Yksi tapa vähentää doxxaajien käytettävissä olevaa tietoa on eritellä verkkoläsnäolosi niin, etteivät eri tilit ja kanavat ole yhteydessä toisiinsa. Tämä on erittäin yksilöllinen prosessi. Pohdi hetken aikaa seuraavia kysymyksiä ja pyri kartoittamaan omat online-verkostosi.

Hengaatko Redditin r/politics-kanavalla, tai vietätkö aikaa keskustelemalla Facebook-tuttavan seinällä? Tykkäätkö tai jaatko usein postauksia radikaaleilta Instagram- tai Twitter-tileiltä? Onko sinulla kuvia tai henkilökohtaisia tietoja työnhakualustoilla? Teetkö ostoksia Etsyssä tai eBayssä? Julkaiseeko joku ystäväsi kuvia sinusta Instagram-tilillesi? Vaatiiko työurasi itsesi mainostamista verkossa? Pidätkö yhteyttä työtovereihin, perheenjäseniin tai aktivistiystäviin saman tilin kautta? Käytätkö osia oikeasta nimestäsi tai syntymäpäivästäsi käyttäjätunnuksissa tai sähköpostiviestissä?

Mikään näistä ei välttämättä ole ongelma sinänsä, mutta yhdessä ne voivat luoda yhteyksiä elämäsi eri osa-alueiden välille.

Pohdi seuraavia asioita:

- Kuinka irrallisia verkossa olevat tilisi ja identiteettisi ovat toisistaan?

- Mikä on julkista? Mikä on yksityistä?
- Mitä julkinen ja yksityinen tarkoittavat kunkin sivuston yhteydessä?
- Mitä voit löytää verkosta etsimällä koko nimelläsi?
- Käytätkö samaa käyttäjätunnusta tai sähköpostiosoitetta useille tileille? Kuuluvatko nämä mitenkään erillisiin elämämpiireihisi? Pohdimmilla eri tavoilla nämä osa-alueet kohtaavat verkon ulkopuolella.
- Voitko olla avoin poliittisista mielipiteistäsi ja tekemisistäsi työpäikkäsi?
- Kuinka julkista aktivismisi on? Puhutko toimittajille? Oletko töissä infoshopissa?
- Suodatatko osan tai kaiken sosiaalisessa mediassa jakamastasi sisällöstä pois sukulaistesi nähtäviltä?
- Löytyykö mistään profiilistasi viittauksia laittomiin tai kiistanalaisiin toimiin?

Tässä on muutama esimerkki siitä, kuinka verkkonäkyvyytesi voi mennä eri sivustoiden kanssa päällekkäin:

Sukulaiset: Kuinka avoin suhteesi sukulaisiin on? Jos tuntematon henkilö saisi haltuunsa tietoa yhdestä sukulaisestasi, mitä hän voisi löytää muista lähipiiriisi tai perheeseesi kuuluvista henkilöistä?

Politiikka: Jaatko tai keskusteletko poliittisista vakaumuksistasi verkossa? Millä alustoilla?

Ystävät ja yhteisö: Jos käytät sosiaalista mediaa, keitä ystäväsi ovat? Entä seuraajasi? Millä tavoin nämä verkkoyhteisöt heijastavat tosielämän yhteisöjäsi?

Harrastukset: Mitä harrastuksia sinulla on? Oletko saanut ystäviä niiden kautta? Onko harrastustesi ympärille rakentunut yhteisöjä, joihin kuulut? Osallistutko näille harrastuksille omistetuisiin internet-yhteisöihin?

Lailliset seikat: Mihin nimiin, puhelinnumeroihin ja osoitteisiin olet sidottu? Ovatko nämä tiedot saatavilla sometiliesi kautta? Entä muiden sivustojen kautta, luvallasi tai ilman?

Ammatillinen ura: Liittykö työhösi verkkonäkyvyys, verkkosivusto tai sometili? Haittäisiko, jos poliittisen toimintasi ja ammatillisen urasi

välillä olisi päällekkäisyyksiä? Liittyykö urasi jollain tavalla poliittiseen identiteettiisi?

Mieti, mitkä ja miten eri elämäsi osa-alueet kohtaavat, missä pystyt niitä erottamaan toisistaan ja mitkä ovat tavoitteesi internetissä ja sosiaalisessa mediassa.

Taktikat

Seuraavaksi käydään läpi, kuinka kartoitat saatavilla olevia henkilökoh-taisia tietojasi ja verkkojälkiäsi, sekä niiden poistamiseksi tarkoitettuja verkkoresursseja.

Aloita julkisesti saatavista tiedoista. Tee itsestäsi verkkohaku ja tee luettelo kaikista some-tileistäsi. Poista vanhat käyttämättömäksi jääneet tilit. Nyt on myös hyvä aika ladata salasananhallintaohjelma, kuten 1Password¹ tai LastPass,² joka auttaa sinua hallinnoimaan yksilöllisiä käyttäjätunnuksia, sähköposteja ja salasanoja.

Poista itsesi tiedonvälittäjien kirjoista

Selvitä, mitä henkilökohtaisia tietojasi hakukoneet pystyvät välittämään muille. Tee haku itsestäsi DuckDuckGossa ja Googlessa. Kokeile hakua incognito-tilassa. Kokeile eri versioita nimestäsi, keskimmäisten nimiesi kanssa ja ilman, lainausmerkeissä ja ilman. Voit aktivoida Googlen hälytystoiminnon, joka ilmoittaa sähköpostitse aina silloin kun nimesi julkaistaan verkossa. Tämä auttaa sinua hahmottamaan kuinka paljon tietojasi sinusta on saatavilla omien verkostojesi ulkopuolisille henkilöille.

Toim. huom. Alkuperäinen artikkeli käsitteli muutaman kappaleen verran Yhdysvalloissa toimivia datavälittäjiä (data brokers), jotka keräävät ja myyvät henkilökohtaisia tietoja. Euroopan alueella toimii myös datavälittäjä, mutta niiden toiminta on vaikeampaa kuin Yhdysvalloissa muun muassa EU:n GDPR-asetuksen takia. Suomen itsenäi-

¹<https://1password.com>

²<https://lastpass.com>

syiden juhlarahasto Sitra julkaisi vuonna 2020 kattavan, Suomen kontekstiin sopivan artikkelin henkilötietojen keräämisestä,³ johon kehotamme tutustumaan. Suomen tietosuojavaltuutetun toimiston nettisivulta löytyy laajasti tietoa siitä,⁴ kuinka voit tarkistaa ja pyytää tietojesi poistamista eri lähteistä.

Poista vanhat tilit

Tee mielellään myös käänteinen haku kaikilla vanhoilla käyttäjä- ja näyttönimillä jotka muistat. Saatat löytää vanhoja tilejäsi. Pitkäksi ajaksi käyttämättömäksi jääneet tilit voivat tehdä sinusta haavoittuvan. Jos niissä on käytössä vanhempi salasana, voivat häiritsijät käyttää kyseisen tilin teknistä tukea saadakseen sinusta enemmän tietoja, joita he pystyvät syöttämään muihin tileihin. Ota kaikki tunnearvokas materiaali talteen ja sulje pysyvästi kaikki käyttämättömät tilit, sillä ne voivat olla täynnä vihjeitä elämästäsi.

Tee hakuja kaikista koskaan käyttämästäsi käyttäjänimistä ja sähköpostiosoitteista. Näin saat selville, mitkä kaikki verkkoalustat ylläpitävät näillä käyttäjänimillä ja sähköpostiosoitteilla rekisteröityjä tilejä. Esimerkiksi nettisivu haveibeenpwned.com auttaa sinua selvittämään tietomurtoja omistamiisi tileihin. Vaihda salasanat välittömästi, jos niitä löytyy.

Vaihda käyttäjänimiä, sähköpostiosoitteita ja salasanoja

Helpoin tapa löytää lisätietoja sinusta on tehdä haku nimelläsi, nimimerkilläsi ja käyttäjänimilläsi. Jos haluat pitää internet-toimintasi osa-alueet erillisinä toisistaan, käytä aina uuden tilin yhteydessä uutta käyttäjätunnusta. Jos sinulla on ammattikäyttöön tarkoitettu verkkosivusto, jossa on käytettävä laillista nimeäsi, varmista, ettet käytä tähän tiliin kytkettyä sähköpostiosoitetta muualla. Sinun on pakko käyttää useita sähköpostitilejä ja käyttäjätunnuksia, jos haluat olla mahdollisimman turvassa. Asioidessasi terveydenhuollon ja valtion verkkopalveluissa käytä tiettyjä

³<https://sitra.fi/julkaisut/henkilodatan-jaljilla>

⁴<https://tietosuoja.fi/yksityishenkilot>

käyttäjätunnuksia,⁵ poliittista elämääsi ja sosiaalista mediaa varten voit luoda omat tunnukset, treffisivustoiden ja verkko-ostoksien yhteydessä asioi eri tunnuksilla ja niin edelleen. Käytä nimimerkkejä ja virheellisiä tietoja kaikilla sivustoilla, jotka edustavat sinua tai näyttävät kuvia sinusta.

Hyvä apu tähän on salasanojen hallintaohjelma, joka käsittelee salasanoja puolestasi tallentamalla kaikkien tiliesi kirjautumistiedot. Suosittelemme LastPassia, jonka voit ladata puhelimeesi ja verkkoselaimeen. Muista aina kirjautua ulos palveluista, vaikka kuinka mieli tekisi jättää itsesi pysyvästi sisäänkirjautuneeksi. Tämä on erityisen tärkeää kahdesta syystä: jotta et unohda salasanaasi, sekä varmistaaksesi, että vaikka joku onnistuisikin saamaan puhelimesi tai tietokoneeseesi haltuun, hän ei pääse käsiksi kaikkiin henkilötietoihisi. Luo uusia sähköpostiosoitteita ja vaihda kaikkien niiden tilien käyttäjänimet, joita et aio poistaa. Voit helposti luoda uusia sähköpostiosoitteita Protonmailin⁶ tai Riseupin⁷ avulla. Sekä 1Password että LastPass auttavat sinua luomaan kaikista turvallisimpia, satunnaisia merkkijonosalasanoja.

Suodata saatavilla olevaa tietoa ja muuta tietosuojasetuksiasi

Kun olet siistinyt kaikki irtonaiset langanpäät, kartoita jäljellä oleva verkkoläsnäolosi. Jos sinulla on sometilejä, käy profiilisi läpi ja pane merkille, minkälaista henkilökohtaista tietoa se sisältää. Voit valita useista eri strategioista sen mukaan, kuinka varovainen haluat olla ja kuinka varma olet siitä, että verkkotoimintasi eri osa-alueet voidaan pitää erillään.

Muutama vaihtoehto:

- Kaikkien kuvien poistaminen itsestäsi, lemmikeistäsi, autostasi, postilaatikostasi, tatuoinneistasi ja kaikesta muusta, joka sisältää tarpeettomia tunnistetietoja—erityisesti julkinen profiilikuvasi.
- Profiilisi henkilökohtaisten tietojen poistaminen tai väärentäminen—merkkää joko virheellinen syntymäpäivä tai jätä kokonaan merkkäämatta, vastaa satunnaisesti kysymyksiin kotikaupungistasi, käymistäsi kouluista ja muista tiedoistasi.

⁵ *Toim. huom.* Suomessa viralliset tahot käyttävät joka tapauksessa useimmiten tunnistautumista verkkopankin kautta.

⁶ <https://protonmail.com>

⁷ <https://riseup.net>

- Kyseenalaisten seuraajien ja ystävien poistaminen. Jos muutat kaikki someasetuksesi yksityisiksi ja tunnet varmasti seuraajapiirisi, kasvosi piilottamiseen on vähemmän syytä. Suosittelen silti, ettet levitä tietoja sijainnistasi tai intiimistä henkilökohtaisesta elämästäsi verkossa. Jos päätät pitää julkisempaa profilia, pidä ystäväsi ja perheesi erillään, äläkä julkaise kuvia heistä tai heidän henkilökohtaisia tietojaan ilman heidän suostumustaan. Muista, että sosiaaliset yhteydet näkyvät sosiaalisten verkostojen ja tiedonkeruusivustojen kautta.

Crash Override Networkin Coach⁸ on hyödyllinen vaihteellinen opas, joka linkittää sinut suoraan käytetyimpien sosiaalisten verkostojen tietosuojasetussivulle. Klikkaa "Let's get started" ja "Strengthen the security of my online accounts so people can't break into them as easily", ja seuraa heidän ohjeistuksiaan. Tämä opas voi auttaa myös muilla verkkoturvallisuuden alueilla. Kun olet käynyt Coach-apuohjelman läpi, suosittelen tutustumaan muihin tarjolla oleviin resursseihin.

Kun luulet olevasi valmis, pyydä ystäväsi esittämään doxxaajaa luomalla sinusta profiilin niiden tietojen perusteella, jotka ovat vapaasti löydettävissä. Onko vielä jotain mitä et pystynyt ennakoimaan, onko jotain päässyt liivahtamaan ohi? Tee haku itsestäsi ja tarkista sinusta saatavilla olevat tiedot aina muutaman kuukauden välein.

Jos sinut on doxxattu

Emme suosittele poliisin puoleen kääntymistä siinäkään tapauksessa, että sinut on doxxattu. Poliisi voi käyttää antamiasi tietoja häirintätekijöistä, mutta se käyttää myös omia tietojasi sekä sinuun julkisesti kytkettyjen henkilöiden ja ryhmien tietoja. Nämä tiedot ovat pysyvästi poliisin kirjoissa, kun ne kerran tallennetaan. Ei ole takeita siitä, ettei poliisi käytä niitä kohdistukseen sinuun valtion sortotoimia.

Jos päätit olla yhteyksissä poliisiin, ole avoin äläkä pyydä radikaaleja ryhmiä tukemaan sinua. Muista ilmoittaa päätöksestäsi kaikille ryhmille, joihin olet yhteydessä. Yleensä poliisi ei tee mitään, tai jopa pahentaa tilannetta.

⁸<https://crashoverridenetwork.com/coach.html>

Tämän oppaan ideana on tarjota sinulle vaihtoehtoja, jotka perustuvat yhteisön tukeen ja voimaannuttamiseen.

Pitäisikö minun kertoa tästä julkisesti?

Lyhyt vastaus: älä reagoi heti julkisesti. Suojaa itsesi ja varoita verkostoissasi olevia henkilöitä ennen kuin teet mitään julkisia eleitä.

Ensimmäinen reaktiosi on luultavasti pyrkimys varoittaa mahdollisimman monia ihmisiä välittömästi julkisella ilmoituksella tai sulkea kaikki verkkotoiminnot. Asian julkiseksi tekeminen tällä tavalla voi tarjota sinulle välitöntä tukea, jos sinulla on sympaattinen yleisö. On kuitenkin mahdollista, että tämä saa vain kiusaajasi aggressiivisemmiksi. On hyvin perusteltua olla varovainen tietojen käsittelyssä heti alusta asti. Tärkeintä on suojata itseäsi ja verkostojasi lisävahingoilta.

Välittömät ilmoitukset voivat monimutkaistaa tietoturvatöitäsi. Riippumatta siitä, pitävätkö sinusta julkaistut tiedot paikkaansa vai ei, kukaan ei todennäköisesti käytä niitä vakavan haitan aiheuttamiseen tarkistamatta ainakin osaa niistä ensin. Kun kerrot doxxauksesta some-tililläsi vahvistat samalla välittömästi, että sinua koskevat tiedot pitävät paikkaansa. Se osoittaa myös, että tiedät missä niitä on julkaistu ja viittaa siihen, että olet kauhuissasi. Tämä edistää kiusaajiesi tavoitteita—he haluavat pelotella ja eristää sinut. Älä vahvista tai kiellä mitään tietoja riippumatta siitä, ovatko ne virheellisiä tai kiusallisia. He haluavat sinusta jonkinlaisen reaktion. Jos viestisi on, että heidän hallussaan olevat tiedot eivät pidä paikkaansa, häiritsijät saattavat päätellä, että he ovat oikeilla jäljillä ja päättävät jatkaa kaivamista. Joskus tehokkain julkinen vastareaktio on, ettei vastaa ollenkaan—älä muuta verkkotoimintaasi, äläkä osoita pelkoa. Tämä tapa reagoida voi parhaassa tapauksessa lähettää viestin, että doxxaus on epäonnistunut.

Kun olet ehtinyt käsitellä tunteitasi ja tilanteesi on vakautunut, voi olla ovelaa kertoa asiasta julkisuudessa ja kenties liittoutua muiden samanlaisessa tilanteessa olevien ihmisten kanssa. Siinä tapauksessa, että julkaisusi aiheuttaa raivoa valkoisten ylivallan kannattajia kohtaan, saatat jopa pystyä järjestämään doxxausvastaisen tempauksen—voit esimerkiksi laittaa rahoituskampanjan pystyyn, jossa osallistujat lupaavat lahjoittaa tietyn summan jokaisesta sinulle tai yhteisöllesi lähetetystä häiritsevästä

sähköpostista! Koska kiusaajasi haluavat eristää sinut, tällainen julkinen tuki voi saada heidät luopumaan pelottelusta. Etsi luovia, joustavia ja strategisia ratkaisuja. Olethan varovainen, että et vaaranna muita tässä prosessissa.

Jos ylpeilet julkisesti kyvyilläsi käyttää esimerkiksi väkivaltaa, esimerkiksi kertomalla aseista, joilla puolustaisit itseäsi, tai liioittelet raivokkuuttasi, saatat kaivaa itsellesi kuoppaa. Yleisesti ottaen ei ole kovin järkevää antaa virheellistä kuvaa itsestään. Yleensä häiritsijöiden kanssa puhuminen joko suoraan tai epäsuorasti ei paranna tilannettasi. Suosittelen tekemään positiivisen lausunnon, jossa alleviivaat arvojesi ja uskomuksiasi sekä kerrot miksi identiteettisi tai näkemyksesi ovat tehneet sinusta doxxauksen kohteen. Sano ääneen, ettet taivu. Näiden häirintäkampanjoiden tarkoituksena onkin juuri lamaannuttaa—sinulla ei ole syytä salata politiikkaasi. Vältä puhumasta tietyistä poliittisista toimista tai ryhmistä riippumatta siitä, oletko mukana niissä vai et.

Heti kun olet tullut doxxatuksi

1. **Älä panikoi.** Soita läheiselle ystävälle ja pyydä apua.
2. **Luo tapahtumaloki** ja pidä kirjaa provokaatioista sekä verkossa että sen ulkopuolella. Tämä on ratkaisevan tärkeää hyökkäyskuvioden tunnistamisessa. Voi olla hyödyllistä verrata näitä muihin doxxatuksi joutuneisiin, jotta voidaan tunnistaa laajempia kaavoja yleisellä tasolla. Näin saatat pystyä tunnistamaan vastustajasi ja heidän järjestöjään.
3. **Laita yksityisviestiä ystävillesi, perheellesi ja erityisen haavoittuville poliittisille verkostoillesi.** Luovuta henkilötietosi muutamille läheisille ystävillesi. Pyydä heitä auttamaan sinua raporttoimalla doxxaavia blogikirjoituksia ja some-julkaisuja häirinnäksi. Kaikilla alustoilla ei ole suojaa antavia käytäntöjä, vaikka häiritsevät julkaisut ja viestit sisältäisivät tarkkoja henkilötietojasi. Joskus doxxaajat tekevät feikki-tilejä käyttämällä haltuunsa saamiaan valokuviasi ja tietojasi. Näistä on yleensä helpompi ilmoittaa. Yritä tehdä se nopeasti, etteivät doxxaajat ehdi saamaan lisää tietoa verkostoistasi esiintymällä sinuna. Sinä, perheesi ja työnantajasi saatatte saada uhkaavia tai häiritseviä puheluja. Kerro heille mahdollisimman nopeasti mitä on meneillään ja pyydä heitä välttämään häiritsijöitä kaikin puolin.

4. **Sulje tiedonkulku.** Jos luet tätä osaa etkä ole suorittanut ennaltaehkäisevän hoidon osaa, ryhdy heti ennaltaehkäiseviin toimenpiteisiin. Lataa salasananhallintaohjelma, kuten 1Password tai LastPass, ja vaihda kaikki salasanasi välittömästi. Käy läpi kaikki mahdolliset some-tilit, verkkotilit ja uutisartikkelit, joissa näkyvää tietoa voit rajoittaa. Varovaisuudessa kuitenkin kannattaa säilyttää tasapaino—yritä siistiä online-jalanjälkiäsi viestimättä kiusaajillesi, että doxxaus oli tehokas tai osui oikeaan kohteeseen. Suojaa sometilejasi esimerkiksi tekemällä ystävälistoista ja muista tiedoista yksityisiä, kunnes olet varma, ettei niistä pysty löytämään henkilökohtaisia tietoja. Julkiset reaktiosi ovat erittäin arkaluonteisia eleitä ja niitä tulee miettiä huolellisesti koko prosessin ajan.
5. **Laadi turvallisuussuunnitelma.** Rekrytoi ystäviä ja sukulaisia tukemaan sinua. Kerro heille, mitä tapahtuu; doxxaus voi olla traumaattinen kokemus. Selviytyäksesi näistä hyökkäyksistä sinun on priorisoitava henkinen ja fyysinen terveytesi. Muiden kanssa käytävät keskustelut saattavat olla vaikeita—varsinkin jos he eivät ymmärrä tämän poliittisen tilanteen monimutkaisuutta, jos he kuulevat ensimmäistä kertaa tietyn viharyhmän toiminnasta tai jos suhteesi ovat poliittisten tai henkilökohtaisten erimielisyyksien vuoksi kireät. Voit myös pyytää tilanteen hyvin ymmärtävää ystävää käymään vaikeammat keskustelut puolestasi.

Jos doxxaus sisältää kotiosoitteesi, ja näyttää siltä että sinuun kohdistuu välitön uhka, sinun on mahdollisesti etsittävä uusi yöpymispaikka. Jos et voi lähteä kodistasi tai muuttaa, kutsu ystäväsi tai paikallinen turvaryhmä luoksesi. Voit pakata ”lähtölaukun” josta löytyy kaikki tarvittava siinä tapauksessa että joudut lähtemään kodistasi lyhyellä varoitusajalla—tämä tuo myös turvallisemman olon.

Uhkien arviointi

Jos et koe olevasi suuressa vaarassa, saatat pystyä kuittaamaan tämän doxxauksen halpana uhkailutaktiikkana, tekemään ilmoituksen häiriköstä ja jatkamaan eteenpäin—varsinkin jos sinuun kohdistettu doxxaus koostuu vapaasti saatavilla olevista tiedoista, tai on lähetetty suoraan ja vain sinulle. Kyse voi olla vain siitä, että joku yrittää saada sinut hermostumaan.

Lisävarotoimiin kannattaa kuitenkin ryhtyä, jos doxxatut tietosi sisältävät arkaluontoisia henkilökohtaisia tietoja, erityisesti sellaisia yksityiskohtia, joihin ei ole helppo päästä käsiksi, tai tietojasi esiintyy julkisessa foorumissa, jossa toiset ihmiset voivat viedä niitä eteenpäin. Tämä pätee erityisesti, jos kuulut jollain tavoin haavoittuvaan ryhmään tai yhteisöön.

Kun saat selville että sinut on doxxattu, on tärkeää selvittää, mitkä tiedot voivat johtaa vakavaan ahdisteluun. Usein doxxaus on tunkeilevemmän offline-häirinnän edeltäjä, tai siihen liittyy uhkaus toimia tietojen perusteella. Tämä voi olla mitä tahansa uhkaavista puheluista perheellesi tai työpaikallesi, aina suoriin tappouhkauksiin.

Joskus on vaikea määrittää, mikä tekee uhkauksesta ”vakavasti otettavan”. Tavallisten häiritsijöiden yleisin taktiikka on lähettää kuumottavia tai pelottavia viestejä mitä tahansa reittiä pitkin jolla voivat sinut tavoittaa —sosiaalisessa mediassa, sähköpostitse, perheenjäsenien kautta, jne. He antavat usein ymmärtää, että heillä on enemmän tietoa kuin mitä heillä todellisuudessa on—tyypillisesti he kertovat toimittaneensa nämä tiedot paikallisille viranomaisille. Tavoitteena on pelotella ja vaikeuttaa toimintaasi. Usein heillä ei ole muuta kun ne samat tiedot, joita he ovat julkisesti levittäneet.

Työnantajasi saattaa saada puheluita, joissa vaaditaan irtisanomista. Toistaiseksi doxxattujen kimppuun hyökkääminen fyysisesti on ollut harvinaista, vaikka niin on joissain tapauksissa käynyt. On mahdollista, että sinua doxxaanneet yrittävät saada tietosi sellaisten ihmisten käsiin, jotka eivät toimi rationaalisesti tai eettisesti. On tärkeää olla varovainen, mutta älä panikoi. Yritä olla ahdistumatta turhaan, ennen kuin tiedät varmasti missä mennään.

Kysy itseltäsi:

- Pitävätkö tiedot paikkaansa? Onko häiritsijöillä koti-, työ- tai perheesi osoitteet? Tietävätkö he missä vietät aikaa tai keitä ystäväsi ovat?
- Oletko vaarassa menettää työpaikkasi, jos julkaistut tiedot tulevat työnantajasi käsiin?
- Tiedätkö missä häiritsijät asuvat? Liikkuvatko he lähellä yhteisöjasi, vai onko pikemmin kyse online-trolleista satunnaisessa foorumilla? Onko sinulla syytä uskoa, että viranomaiset ovat kiinnostuneita

näistä tiedoista? Onko tietojasi jaettavana paikallisissa oikeistolaisissa uutislähteissä, jonka seurauksena useat vieraat vihamieliset henkilöt pystyvät tunnistamaan kasvosi?

- Onko heillä kiusallisia tai yksityisiä kuvia sinusta?
- Onko olemassa tietoja, jotka sitovat sinut rikolliseen toimintaan ja voisivat johtaa pidätykseen?

Ratkaisuja

Tässä on joitain tapoja torjua doxxaukseen liittyviä vaaroja:

- Luo itsepuolustus suunnitelma, ilmoittaudu mukaan itsepuolustus-kursseille
- Ilmoita tapahtuneesta doxxauksesta tarpeellisille ihmisille ja ryhmille —työpaikalle, tovereille, kämppekavereille, perheelle.
- Keskustele peloistasi ihmisten kanssa, joihin luotat.
- Ole yhteyksissä ja pyydä neuvoja ihmisiltä, joilla on kokemusta doxxauksesta.
- Hanki asianajaja, jos olet huolissasi siitä, että sinua koskevat tiedot voivat kiinnostaa valtiota.
- Ota yhteyttä paikalliseen antifasistiseen ryhmään—he pystyvät mahdollisesti auttamaan sinua tunnistamaan häiritsijät, jos nämä lähettävät viestejään valetileiltä.

Kun keskustelet työpaikalla ja perheen kanssa

Tämä keskustelu voi olla erittäin vaikea, varsinkin jos sinulla on kireät suhteet perheeseesi. Pyydä tarvittaessa ystävää auttamaan tai tukemaan sinua jälkikäteen.

Mieti, kuinka usein olet valmis olemaan haavoittuvainen perheesi kanssa ja kuinka paljon sinulla on jatkossa mahdollisuuksia jatkaa keskustelua. Jos on tarpeen puhua perheenjäsenten kanssa, mutta on todennäköistä, ettei saa kuin vain yhden mahdollisuuden, voit valmistautua heidän reaktioihinsa harjoittelemalla ystävän kanssa. Jos sinulla on jatkuva, keskusteleva, luottamuksellinen suhde, voit selittää heille tilanteen lyhyemmissä pätkissä yhden pitkän istunnon sijaan. Arvioi, kuinka paljon aikaa ja kuinka paljon huomiota tulet heiltä saamaan.

Ihmisille, joiden kanssa en halua käydä poliittista keskustelua, olen itse usein kertonut että ”minulla on stalkkeri”—tämä sanoitus saattaa riittää selittämään tilanteen vakavuuden ja yksityisyyden tarpeen. Voi kuitenkin olla vaivan arvoista olla rehellinen siitä, mitä oikeasti tapahtuu. Tämä voi auttaa rakentamaan vahvempia ihmissuhteita ja tuomaan doxxausta esiin yleisenä ilmiönä. Samalla rohkaistaan muita ottamaan verkkoyksityisyys vakavasti; varsinkin heitä, jotka eivät ole tulleet ajatelleeksi, että näin voisi tapahtua heille tai jollekulle heidän tutulleen. Useimmat ihmiset reagoivat pelolla ja myötätunnolla, vaikka joskus he toki saattavat ehdottaa tai jopa vaatia, että ilmoitat asiasta poliisille.

Lähestymistapoja on monta, eikä mikään ole se yksi ja ainoa. Omasta puolestani jouduin pakottamaan konservatiivisen äitini lupaamaan, ettei hän ottaisi yhteyttä poliisiin. Vetosin oikeuteeni henkilökohtaiseen turvallisuuteen ja itsemääräämisoikeuteen tämän tapauksen uhrina. Pyysin häntä kunnioittamaan toiveitani muistuttamalla häntä siitä, että poliisi ei pysty reagoimaan tällaiseen kohdennettuun häirintään juuri mitenkään—puhelu heille olisi vain asettanut minut tarkastelun alaiseksi, koska minua syytettiin rikollisesta toiminnasta. Tällaiset keskustelut voivat olla erittäin vaikeita, mutta ne ovat usein tarpeellisia. Muistuta ystäviäsi ja perhettäsi olemaan vastaamatta puheluihin, sähköposteihin tai sosiaalisen median viesti- tai kaveripyyntöihin.

Täältä⁹ löydät oppaan jossa kerrotaan, kuinka kannattaa keskustella asiasta työnantajasi kanssa.

Kun puhut ystävillesi ja perheellesi, muista nämä asiat:

- Doxxaajien tavoitteena on rasittaa suhteitasi ja pilata elämäsi. Älä anna heidän onnistua tässä. Kerro perheellesi, että paras tapa tukea sinua on kieltäytyä antamasta periksi heidän taktiikalleen.
- Älä osoita sormella anarkisteja ja antifasisteja, äläkä väitä, että sinut on valittu kohteeksi ilman syytä. Tämä ei auta sinua, jos syytä sittenkin ilmaantuu—se myös delegitimoi ja vaarantaa entisestään ne, jotka eivät voi etäännyttää itseään anarkistisesta politiikasta.
- Älä anna kenenkään syyttää sinua tapahtuneesta, olipa sitten kyse politiikastasi tai oletetusta vastuuttomuudestasi, jonka takia olet

⁹<https://crashoverridenetwork.com/employers.pdf>

joutunut ”tähän tilanteeseen”. Taistelu paremman maailman puolesta sisältää haasteita. Se on itse asiassa ansiosi, että ponnistuksesi ovat saaneet tällaisen reaktion aikaiseksi.

- Ehdota konkreettisia tapoja, joilla voit auttaa heitä ymmärtämään tilanteen ja suojelemaan itseään. Lähetä heille tämä artikkeli tai luettelo resursseista; tarjoudu auttamaan heitä suojaamaan sometilejäänsä, jos he eivät ole teknisesti taitavia.
- Kerro, mihin he voivat valmistautua—häiritsevät puhelut, sähköpostit, ehkä naapurit tulevat saamaan viestejä sinusta. Valmista heidät pahimpaan mahdolliseen skenaarioon, mutta painota, että se on epätodennäköistä.
- Varmista että he tietävät minkälaista tukea sinä tarvitset heiltä.

Elämä jatkuu

Hengitä syvään. Älä syytä itseäsi. Doxxaus voi olla syvästi häiritsevä ja järkyttävä asia, joka myös lisää akuuttia stressiä elämässäsi. Yhtäkkiä jossain saattaa olla ihmisiä, jotka tietävät miltä näytät, etkä tiedä keitä he ovat. Joskus doxxatuista tiedoista tulee pysyvä osa internetiä, esimerkiksi silloin kun nimesi syötetään hakukoneisiin. Tämä voi vaikuttaa työllistymismahdollisuuksiisi. Joskus doxxauksen kautta noussut huomio ei aiheuta yhtään mitään, mutta aina on mahdollista, että joku yrittää jatkaa siitä mihin edellinen doxxaaja jäi.

Ennen kuin olet varma, että hetkesi parrasvaloissa on ohi, saatat joutua tekemään joitakin muutoksia elämässäsi. Kysy itseltäsi: ”Millaista elämää haluan elää? Kuinka voin hallita ahdistustani? Onko tapoja, joilla pystyisin hyväksymään julkisuudessa olemista? Miten voin tuntea oloni turvalliseksi ottaessani riskejä ja ollessani taas aktiivinen?” Varsinkin poliittisten jännitteiden kiristyessä voi olla tärkeää ryhtyä äärimmäisempiin turvatoimiin.

Tässä on joitain toimenpiteitä, joihin voit turvautua:

- Älä anna kenenkään valokuvata sinua, ellet luota että he käsittelevät kuviasi haluamallasi tavalla. Tämä voi aiheuttaa kiusallisia keskusteluja, etenkin perhetapahtumissa tai ammatillisissa tilanteissa. Ole tietoinen siitä, kuka esiintyy kuvissa kanssasi; kerro heille, että kuvassa esiintyminen kanssasi saattaa herättää ei-toivottua huomiota. Voi olla hyödyllistä myös harjoitella tätä keskustelua etukäteen.

- Asenna kotiin turvakameroita.
- Pidä kirjaa kaikesta kokemastasi häirinnästä.
- Jos muutat, älä päivitä osoitettasi. Yritä pitää kiinni vanhasta ajokortistasi tai henkilöllisyystodistuksestasi ja nouda postisi paikallisesta postilokerosta. Tee valintoja osoitetietojesi jakamisen suhteen: kun rekisteröidyt palveluihin verkossa ja muutoin, mieti milloin käytät oikeaa osoitettasi, milloin väärennettyä osoitetta ja milloin jätät osoitteesi kokonaan pois.
- Käytä nimimerkkejä verkossa ja tarvittaessa myös henkilökohtaisissa kohtaamisissa. Älä käytä samaa nimeä jatkuvasti, vaan aina välillä uusia nimimerkkejä.
- Kun lähdet poliittisiin tapahtumiin mukaan, varsinkin jos et peitä kasvojasi, pidä mielessä mitkä ryhmät, paikat tai henkilöt saattavat assosioitua sinuun, jos niitä nähdään tai valokuvataan sinun rinnallasi.
- Opettele itsepuolustusta, käy kursseilla. Tämä voi sisältää asekoulutusta, mutta sen tulisi ehdottomasti sisältää puolustautumiseen ja aseistariisuntaan liittyviä tekniikoita.
- Käänny terapeutin puoleen selvittämään kokemiasi traumoja.
- Auta ystäviäsi ja perhettäsi ymmärtämään verkkoturvallisuuden tärkeyttä.
- Keskustele rehellisesti ulkopuolisten ihmisten kanssa, jotka eivät kuulu poliittiseen piiriisi. Saatat yllättyä heidän empatiakyvyistään.

Toim. huom. Vaikka viranomaisiin kannattaa suhtautua äärimmäisen kriittisesti, voit pahimmissa tapauksissa joutua tahtomattasikin asioimaan heidän kanssa jos olet doxxaamisen uhri. Jos joudut esitutkintaan tai oikeudenkäyntiin, natsit tai muut poliittiset viholliset saattavat saada tietoonsa nimesi tai muita tietojasi, vaikka et saisi-kaan tuomiota. Tässä tapauksessa voit hakea turvakiellon, mikä tekee sinut ja osoitteesi näkymättömäksi. Tämä vaikeuttaa elämäsi monella tavalla; joudut hakemaan postisi Poste Restante -palvelusta, et voi ostaa tavaroita luotolla helposti koska myös luottotiedosi salataan, ja

työhastatteluissa työnantaja voi ihmetellä kun tietojasi ei löydy. Turvakielto on kuitenkin yksi vaihtoehto jos olet uhattu.

Voit myös kieltää tietojesi luovutuksen näillä sivuilla:

- Väestötietojärjestelmästä Suomi.fi-sivun¹⁰ henkilötiedot-osiossa. Voit kieltää tietojen luovutuksen väestötietojärjestelmästä siten, että tietojasi ei luovuteta suoramarkkinointiin (sisältää markkinatutkimukset ja mielipidetutkimukset), henkilömatrikkeleihin, sukututkimuksiin tai asiakasrekistereiden päivityksiin.
- Puhelinnumerosi ja osoitetietosi näkymisen numerialuepalveluissa voit salata oman operaattorisi kautta.
- Traficomin liikenteen rekisterit ovat lähtökohtaisesti julkisia. Halutessaan omien tietojen luovuttamista voi kuitenkin rajoittaa. Voit tehdä salaamispyynnön kirjautumalla osoitteessa.¹¹

Huolimatta siitä, missä määrin sinua mahdollisesti ahdistelevat ihmiset saavat sinut tuntemaan olosi eristäytyneeksi, et ole tässä yksin. Yhteisönä meidän on suojeltava toisiamme ja online-verkostojamme häirinnältä, vangitsemiselta, poliittiselta väkivallalta ja pelottelulta. **Yhdessä pystymme tähän.**

¹⁰<https://suomi.fi/omat-tiedot/henkilotiedot>

¹¹<https://asiointi.traficom.fi/oma-asiointi>

Tässä oppaassa kerrotaan vaihe vaiheelta, kuinka suojautua verkkohäiritsijöiltä, miksi se on tärkeää, ja mitä tehdä, jos joudut ”doxxauksen” kohteeksi. Doxxaus tarkoittaa henkilökohtaisten tietojesi julkaisemista.



No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

Depending on your context, possession of certain documents may be criminalized or attract unwanted attention. Be careful about what zines you print and where you store them.