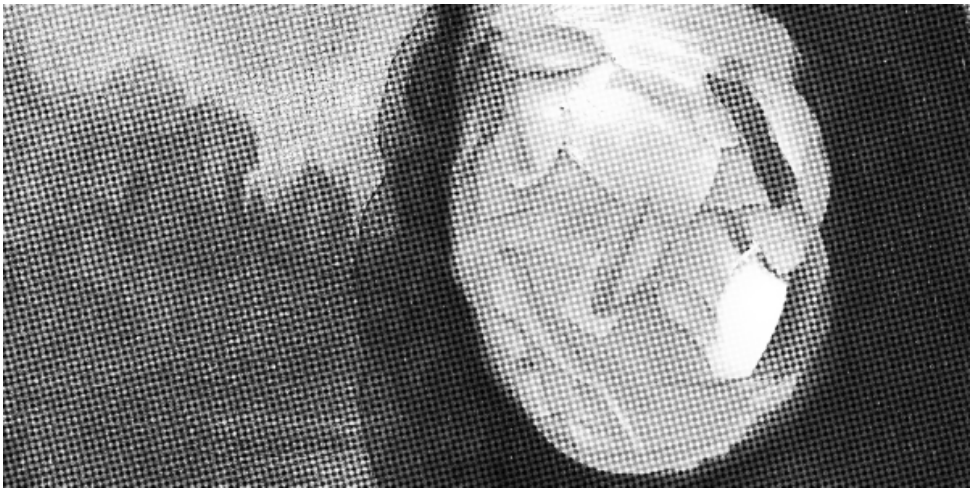
Doxcare

Prevención y asistencia posterior para las víctimas de doxeo y acoso político



Doxcare: Prevención y asistencia posterior para las víctimas de doxeo y acoso político

Texto original en inglés

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

Traducción al español

Ediciones Extáticas

edicionesextaticas.noblogs.org/post/textos-y-traducciones/introduccion-a-la--cultura-de-la-seguridad

Maquetado

No Trace Project

notrace.how/resources/es/#doxcare

Esta guía detallada explica cómo protegerse de los acosadores en línea, por qué es importante hacerlo y qué hacer si eres víctima de «doxeo»—la publicación de tu información privada.

Contenido

¿Qué es el Doxeo?

Doxear significa publicar la información privada de una persona con el objetivo de exponerla e intimidarla. Esto puede provocarle un daño físico, emocional y económico. Se hace con la intención de disuadir al objetivo de actuar y humillarlo por sus ideas y valores. Por ello, es importante plantearnos seriamente la cultura de la seguridad antes de que nos doxeen —antes de que tengas motivos para temer de un posible doxeo. Normalmente el doxeador esperará a recolectar la información necesaria antes de exponerla. Es posible que ya estés siendo vigilado sin saberlo hasta que ya sea demasiado tarde.

Seas un activista público bastante reconocido, o alguien que no se entromete mucho, deberías proteger todas tus redes sociales y otras esferas de tu vida—incluso si crees que no estás haciendo nada que merezca atención. Mantener una buena práctica protege a tus amigos, tu familia y tu comunidad. Es común que grupos derechistas incluyan en sus teorías aquellos que son queer o trans, que «parece un izquierdista», tocan en bandas, van a eventos o frecuentan espacios radicales. La información no debe ser correcta o justificada para que alguien te tenga como objetivo. Lo único que necesita un acosador es una sola pieza de información para empezar a indagar más detalles en la red.

Ser consciente de los rastros de información que dejas en internet puede protegerte tanto de las fuerzas del orden como de los acosadores. Ahora que la vigilancia impuesta por el Estado es cada vez más sofisticada, y que los directos en redes sociales se han normalizado en las protestas, ya no basta con llevar un simple tapabocas. En Junio de 2020 en Philadelphia, los investigadores identificaron a una mujer con tan sólo una imagen difuminada de ella. Siguieron un rastro de migas, aparentemente minucioso, que incluía una compra en Etsy, su cuenta de Twitter y su página de trabajo profesional. El Servicio de Aduanas y Protección de Fronteras ha empezado a rastrear las redes sociales públicas. Proteger tu presencia en internet puede hacerte sentir más seguro al actuar fuera de estas redes.

Más vale prevenir que curar

El mejor momento para empezar es ahora, pues después de haber sido doxeado, probablemente, seas incapaz de eliminar la información expuesta incluso tratando de quitarla de la red.

Hay muchas maneras de tratar este tema. Obviamente, la mejor forma de asegurarnos de que nadie pueda encontrar información sobre ti es no tener nada al alcance de nadie—pero no todo el mundo puede eliminar su presencia de internet, sea por trabajo, familia, u otras responsabilidades. En algunos casos, existen razones estratégicas para mantener cierto tipo de persona online; por ejemplo, tener un perfil en alguna red social de hace mucho tiempo, creíble pero innocuo, puede ser útil para los no-ciudadanos estadounidenses que tratan de cruzar la frontera. Afortunadamente, hay muchas formas de compartimentar las distintas esferas de tu vida, de crear un perfil público si lo necesitas y de adoptar prácticas que te ayuden a ti y a tus amigos a sentiros capacitados para seguir actuando en tu comunidad. Este proceso puede resultar tedioso. Requiere tiempo y energía. Recomiendo realizar esto con amigos, compañeros de piso o familiares para que te ayuden en algunos de los aspectos difíciles o aburridos.

Mantener esferas separadas

Si no puedes borrar tu huella digital por completo de Internet, aún puedes preservarse una relativa privacidad manteniendo distintas esferas[1] de actividad online y limpiando las cuentas olvidadas o de uso poco frecuente.

Es probable que tengas más de una presencia online. Esto incluye redes sociales, tableros de mensajes, sitios de trabajo, cuentas de correo electrónico—cualquier cosa en la que necesites entrar. A menudo, en el doxeo, la información se triangula a partir de muchas fuentes distintas. Una forma de reducir la cantidad de información disponible para los doxeadores es compartimentar estas esferas para que no estén conectadas entre sí. Este es un proceso completamente individualizado; tómate un tiempo para considerar las siguientes preguntas y mapear tu propia esfera online.

---

[1] El concepto de esferas aquí empleado se lo debemos a Smiling Faces Collective.[2]

[2] https://smilingfacecollective.github.io/guide-to-preventing-doxxing

¿Pasas las horas mirando foros como r/politics o debatiendo en el muro de un conocido de Facebook? ¿Interaccionas con alguna cuenta radical de Instagram o Twitter? ¿Tienes imágenes o información personal en tableros de ofertas laborales? ¿Compras por Etsy o eBay? ¿Uno de tus amigos publica una foto tuya en su cuenta de Instagram? ¿Tienes que promocionarte online para el tipo de trabajo al que te dedicas? ¿Hablas con tus compañeros de trabajo, familiares, y amigos activistas con la misma cuenta? ¿Utilizas parte de tu nombre real o tu fecha de nacimiento para los nombres de usuario o los correos electrónicos?

Cada uno de estos no tiene porqué ser un problema como tal, pero juntos pueden crear vínculos entre las diferentes esferas de tu vida.

Pregúntate:

- ¿Cuán separadas están cada una de estas cuentas/identidades?
- ¿Qué es público? ¿Qué es privado?
- ¿Qué significa público-privado en el contexto de cada sitio?
- ¿Qué puede encontrarse al buscar tu nombre legal?
- ¿Utilizas el mismo nombre de usuario o correo electrónico en múltiples cuentas? ¿Se cruzan en tus distintas esferas de vida? Tómate tu tiempo para pensar en la forma en que todas estas esferas se superponen fuera de Internet.
- ¿Tu trabajo te permite hablar abiertamente de tu política?
- ¿Cuán público es tu activismo? ¿Hablas con periodistas? ¿Trabajas en una infoshop?
- ¿Filtras parte o todo el contenido de tus redes sociales de tus familiares?
- ¿Hay referencias a actividades ilegales o controvertidas en un perfil determinado?

He aquí algunos ejemplos de cómo tu presencia online puede superponerse en distintos sitios:

Familiares: ¿Hasta qué punto es abierta la relación entre tú y tus familiares de sangre/legales? Si un extraño tuviera información sobre una sola persona de esta red, ¿qué podría descubrir sobre las demás?

Política: ¿Discutes o publicas sobre tus pensamientos políticos online? Si es así, ¿en qué redes sociales?

Amigos y comunidad: Si tienes redes sociales, ¿quiénes son tus amigos? ¿Tus seguidores? ¿De qué formas tus comunidades online reflejan tus comunidades en la vida real?

Hobbies: ¿Qué hobbies tienes? ¿Tienes amigos y comunidad a través de ellos? ¿Eres parte de alguna comunidad de Internet dedicada a esos hobbies?

Legal: ¿Quién eres en papel? ¿A qué nombres, números de teléfono, direcciones estás vinculado? ¿Alguna de tus cuentas incluye esta información? ¿Lo hace algún otro sitio (probablemente sin tu permiso)?

Profesión: ¿Tu trabajo implica una presencia online, un sitio web o una cuenta en alguna red social? ¿Habría algún problema si tus políticas se superpusieran con tu profesión? O, ¿tu profesión está de alguna forma vinculada a tu identidad política?

Tómate el tiempo necesario para considerar el punto donde se cruzan, cuáles son tus objetivos online y dónde puedes separar estas esferas.

Tácticas

Hablemos de cómo descubrir qué tipo de información nuestra está disponible, cómo identificar y eliminar los rastros, y qué herramientas online existen para eliminarlos.

Empieza con lo que esté disponible públicamente. Búscate en Google y haz una lista de todas tus redes sociales. Elimina las cuentas antiguas que ya no utilices. También es un buen momento de descargarse un *password manager* como 1Password[3] o LastPass[4] para facilitarte en manejar nombres de usuario, correos electrónicos y contraseñas concretas.

[3]https://1password.com
[4]https://lastpass.com

Elimina los sitios de espionaje/brókers de información

Averigua qué información puede encontrar la gente sobre ti utilizando un motor de búsqueda. Búscate a ti mismo en DuckDuckGo y Google. Intenta hacerlo en modo incógnito. Prueba con distintas versiones de tu nombre, con o sin tu segundo nombre y entre comillas. Puedes configurar Google Alerts para que te envíe un correo cada vez que tu nombre sea publicado en Internet. Esto te dará una perspectiva de cuanta información sobre ti hay disponible online a la gente que no es de tu red (de confianza).

Después de esta búsqueda inicial, dales una ojeada a todos los sitios de brókers de información (Data Brokers) que se benefician del comercio de datos personales. También te animo a que elimines al mismo tiempo a tus familiares más cercanos. Este proceso puede ser arduo; estos sitios intentan dificultar al máximo la eliminación de información sobre uno mismo. Hay algunas de las que no puedes borrarte—por ejemplo, si te has registrado para votar y aún vives en esa dirección. (Este es otro motivo por el que la gente decide no votar).

Los sitios de alojamiento con más tráfico incluyen: Been-verified, CheckPeople, Instant Checkmate, Intelius, PeekYou, PeopleFinders, PeopleSmart, Pipl, PrivateEye, PublicRecords360, Radaris, Spokeo, USA People Search, TruthFinder.com, Nuwber, OneRep, y FamilyTreeNow. Recomiendo empezar por estos buscando cada uno de ellos en esta página web,[5] que tiene una guía para excluirse de prácticamente todos los DataBrokers. Si tienes más dinero que tiempo, puedes pagar por un servicio llamado Delete Me[6] para que eliminen tu información, aunque normalmente recomiendo este servicio si ya has sido doxeado.

Elimina tus antiguas cuentas

Cuando te buscas a ti mismo en un motor de búsqueda online, es probable que también te encuentres con cuentas antiguas. Puede ser beneficioso realizar una búsqueda inversa utilizando todos los nombres de usuario y alias antiguos que puedas recordar. Cuentas que no hayas utilizado en mucho tiempo pueden hacerte vulnerable porque si utilizaste en ellas una

[5] https://joindeleteme.com/blog/opt-out-guides

[6] https://web.archive.org/web/20210804023430/https://onlinesos.org/blog/i-tried--abine-delete-me-to-get-my-info-off-data-broker-websites

antigua contraseña, pueden probar el soporte técnico de esa cuenta para obtener más información sobre ti, y que pueden usar para otras cuentas. Descarga todo el material que tengas con valor sentimental y cierra indefinidamente todas las cuentas que ya no utilices. Éstas pueden estar llenas de pistas sobre tu vida.

Primero, entra en esta página web,[7] que busca en cientos de plataformas nombres de usuario específicos, y busca todos los posibles nombres de usuario y correos electrónicos que hayas utilizado. Esto te dirá qué plataformas tienen cuentas con ese nombre.

Segundo, entra en esta página[8] y escribe el dominio del sitio web. Esta página web archiva una gran variedad de sitios webs existentes, clasificando por cuán sencillo o difícil puede ser borrar una cuenta, además de proporcionar el enlace a la página de «eliminar perfil» de cada sitio.

El sitio haveibeenpwned.com facilitará averiguar si hay alguna brecha de información en alguna de tus cuentas. Si la hay, toma medidas inmediatas para cambiar las contraseñas.[9]

Cambia nombres de usuario, direcciones de correo electrónico y contraseñas

El método más sencillo de que alguien encuentre más información sobre ti es buscar tu nombre, tus alias y tu nombre de usuario. Con el fin de mantener las esferas de actividad en Internet separadas, utiliza siempre un nuevo nombre de usuario cuando crees una cuenta. Si tienes una página web profesional para el trabajo que requiera de tu nombre de usuario, asegúrate que el correo electrónico utilizado para esa cuenta sea destinado para ese único propósito. Es posible que acabes teniendo un sinfín de correos electrónicos y nombres de usuario. Por ejemplo, yo tengo una sola para todas mis cuentas médicas y gubernamentales, otra para mis compras online, otra para mi vida política, otra para mis redes sociales, otra para

[7] https://namechk.com

[8] https://backgroundchecks.org/justdeleteme

[9] *Nota de traducción (NdT):* Realizar este proceso de revisión de forma trimestral, cada dos semanas, cada mes, o las que consideres necesarios, pero nunca confiar en una simple y única revisión.

los sitios de cita, etc. Utilizo alias e información falsa para todos los sitios web que me representan o muestran fotos mías.

Un gestor de contraseñas es una gran ayuda para esto, pues almacenará los inicios de sesión de todas tus cuentas. Recomiendo LastPass. que puedes descargar en tu móvil y navegador. Sería tentador dejar la sesión abierta permanentemente, pero asegúrate siempre de cerrar la sesión cuando termines de usarla. En concreto, para no olvidar la contraseña maestra —y también para asegurarte de que incluso si alguien consigue acceder a tu móvil u ordenador, no puedan tener acceso a tus datos personales. Aprovecha este momento para crear nuevos correos electrónicos y cambiar los nombres de usuario de todas las cuentas que no vayas a eliminar. Puedes crear fácilmente nuevos correos electrónicos utilizando Protonmail.[10] Tanto 1Password como LastPass pueden ayudar a generar contraseñas de cadenas aleatorias, que son las más seguras.

Cura lo que está disponible y cambia tu configuración de privacidad

Una vez que hayas eliminado todos los cabos sueltos, ojea lo que decidiste conservar y lo que se puede encontrar de ahí. Si conservas alguna cuenta en las redes sociales, revisa tu perfil y anota lo que la gente puede encontrar sobre ti. Puedes elegir una entre una serie de estrategias sobre cómo enfocar esto, dependiendo lo cauteloso que quieras ser y lo seguro que estés de que es posible mantener tus diferentes esferas de actividad en Internet diferenciadas.

Algunas de las opciones incluyen:

- Eliminando todas las fotos en las que salgas tú y tus mascotas, tu buzón, tus tatuajes, y todo aquello que incluya información innecesaria pero identificatoria—especialmente de tu foto de perfil pública.
- Borrando o falsificando cualquier detalle personas de tu perfil—proporciona una fecha de nacimiento falsa o, directamente, no la des, elige una localización falsa de tu ciudad natal, de las escuelas a las que fuiste, y más información por el estilo.
- Eliminando seguidores o amigos dudosos. Si cambias toda la configuración de tus redes sociales a privado y te sientes seguro con tu

[10]https://protonmail.com

depurada lista de seguidores, hay menos motivos para esconder tu cara. Sigo recomendando mantener los detalles de tu localización y tu vida personal íntima fuera de Internet. Recuerda que sólo estás tan seguro como la persona más abierta de tu vida. Si decides ser más público, mantén a tus amigos y familiares por separado, sin publicar fotos de ellos o información personal suya sin su consentimiento, y recuerda que las conexiones sociales son visibles a través de las redes sociales y los sitios web de recopilación de datos.

El C.O.A.C.H[11] de Crash Override Network es una guía útil paso a paso que te enlaza directamente con la página de configuración de la privacidad de muchas redes sociales. Haz click en «Let's Get Started» y en «Strengthen the security of my online accounts so people can't break into them as easily», y sigue sus guías para todas las principales compañías de redes sociales. Esta guía también puede ayudar con otros aspectos de la seguridad online, así que después de hacer eso, te recomiendo que termines las ayudas del Coach y compruebes qué otros recursos ofrecen.

Cuando creas haber terminado, pídele a un amigo que se haga pasar por un «doxeador» y que intente crear un perfil basado en la información que pueda encontrar sobre ti para comprobar que no se te haya escapado algo por alto. Puede ser importante comprobar periódicamente lo que se puede encontrar buscando tu nombre cada pocos meses.

Si has sido doxeado

No recomendamos dirigirse a la policía cuando hayas sido (alguna vez) doxeado. La policía puede utilizar esta información proporcionada sobre los acosadores, pero también utilizará esta información obtenida sobre ti y otros individuos y grupos en los que hayas estado asociado públicamente. Una vez que esta información está archivada, estará permanentemente en sus manos, y no hay garantía de que no la utilicen para atacarte a ti o a otros mediante la represión del Estado.

Si decides implicar a la policía, por favor sé transparente y no preguntes a ningún grupo radical que te apoye. Asegúrate de informar de tu decisión

[11] https://crashoverridenetwork.com/coach.html

a cualquier grupo en el que estés involucrado. Generalmente, la policía no hará nada o empeorará de más la situación. La idea de esta guía es proporcionarte alternativas basadas en el apoyo de la comunidad y el empoderamiento.

¿Debería hacerlo público?

Respuesta breve: No reacciones inmediatamente en público. Tómate tu tiempo para asegurarte y alertar a tus redes en privado antes de reaccionar públicamente.

Tu primer impulso puede ser alertar a tanta gente como sea posible de inmediato con un anuncio público, o cerrar todas tus redes. Hacerlo público puede proporcionarte un apoyo inmediato si tienes una audiencia solidaria, pero conlleva el riesgo de que aumenten las agresiones de los acosadores. Hay buenos argumentos para ser cuidadosos con la información al principio. Lo más importante es tomar medidas para protegerte a ti y a tus redes contra un mayor daño.

Los anuncios inmediatos pueden complicar tus esfuerzos de seguridad. Tanto si la información publicada sobre ti es cierta o no, es probable que nadie la utilice para causarte un daño grave sin confirmar primero al menos parte de ella. Publicar en una de tus cuentas confirmando tu doxeo aprueba inmediatamente que la información sobre ti es exacta; también indica que has visto dónde se ha publicado y sugiere que estás aterrorizado. Esto favorece los objetivos de tus acosadores. Quieren intimidarte y aislarte.

No confirmes ni niegues ninguna de las informaciones que han desenterrado sobre ti, independientemente de que sean falsas o embarazosas. Buscan una reacción. Si les haces saber que lo que están publicando es incorrecto, pueden llegar a la conclusión de que van por buen camino y que sólo tienen que seguir indagando. A veces, una de las respuestas públicas más efectivas es no responder a nada—no hagas ningún cambio importante en tus hábitos de publicación ni muestres miedo. Esto puede enviar la señal a tu doxeador de que no dio en el blanco, y que el ataque fue un fracaso.

Una vez que hayas tenido tiempo para procesar tus sentimientos y asegurar tu posición, sería estratégico hacerlo público y quizás unirte a otras personas que estén en una situación similar. Puedes aprovechar la indaga-

ción pública (por los supremacistas blancos) para crear una campaña que disuada el uso del doxeo—por ejemplo, ¡haz una campaña de financiación con promesas de dar dinero por cada correo electrónico de acoso que tú u otras personas de tu comunidad hayáis recibido! Dado que tus acosadores quieren aislarte, un apoyo público como éste puede disuadir de una mayor intimidación. Intenta ser creativo, resistente y estratégico. Sé cuidadoso de no poner en peligro a nadie más en este proceso.

Al hacer declaraciones públicas, si presumes o alardeas de tus habilidades, de tu capacidad para emplear violencia, de las armas que dispones para defenderte, o exageras tu ferocidad, puedes morder más de lo que puedes masticar. Por norma general, no es buena idea tergiversar la información sobre ti. Hablar directa o indirectamente con los acosadores no suele mejorar las cosas. Recomiendo hacer una declaración positiva afirmando tu ética y tus creencias, describiendo cómo tu identidad o tus ideales te han convertido en un objetivo, pero manteniendo que, aunque estas campañas de acoso pretenden acobardarte, no lo harás, porque no tienes razón alguna para ocultar tu política. Evita hablar de acciones o grupos concretos, estés o no involucrados con ellos.

Inmediatamente después de ser doxeado

1. **No temas.** Llama a un amigo cercano para que venga a darte apoyo.
2. **Crea un registro de incidentes** y mantén un registro de las provocaciones tanto online como fuera de Internet. Esto es crucial para identificar los patrones de los ataques. Puede ser útil compararlos con los de otros organizadores para identificar patrones más amplios y así poder identificar a tus adversarios y sus organizaciones.
3. **Avisa a tus amigos, familiares y redes políticas sensible por privado.** Encarga a algunos amigos en los que confíes tu información personal a que te ayuden a denunciar las publicaciones en redes sociales y blogs que te doxen, identificándolas como acoso. Repite este proceso las veces que sean necesarias. Algunas plataformas carecen de políticas que te protejan, incluso si estas publicaciones incluyen información personal precisa, incluso si te ponen en peligro. A veces, los doxeadores usarán tus fotos e información para crear cuentas impostoras. Suele ser más sencillo reportarlas como falsas; intenta

hacerlo rápidamente para evitar que obtengan más información de tus redes haciéndose pasar por ti. Es posible que tú, tu familia y tus compañeros de trabajo comiencen a recibir llamadas telefónicas amenazantes o de acoso. Hazles saber lo que está ocurriendo tan pronto como puedas para que no se relacionen con los acosadores.

4. **Detén el flujo de información.** Si estás leyendo este apartado sin haber hecho los cuidados preventivos expuestos, comienza este proceso. Descarga un gestor de contraseñas como 1Password o LastPass y cambia de inmediato todas tus contraseñas. También puedes pagar por un servicio llamado Delete Me que eliminará gran parte de tu huella digital de los sitios de espionaje [Snoop Sites] que recogen y monitorean información personal. Este servicio se encargará de la información agregada por los brókers de datos [Data Brokers], pero no de las redes sociales, las cuentas web, los artículos de noticias o los registros de arresto que pueda tener—estos deberán ser manejados por uno mismo. Es importante equilibrar la hemorragia de información mientras, al mismo tiempo, no se alerta a los acosadores de que el doxeo fue efectivo o hizo diana. Intenta asegurar tus cuentas en las redes sociales haciendo que las listas de amigos y la información sean privadas para proteger tus redes hasta que estés seguro de que no ofrecen información personal vulnerable a quienes estén dispuestos a indagar en ella. Cómo reaccionas públicamente es una situación muy delicada y debe manejarse con cuidado durante todo este proceso.
5. **Establece un plan de seguridad.** Recluta a amigos y familiares para que te den soporte. Hazles saber qué está pasando; el doxeo puede ser traumático y debes priorizar tu salud mental y física para poder superar estos ataques. Estas conversaciones pueden ser difíciles—especialmente si no entienden los matices de este momento político, si es la primera vez que oyen hablar de un grupo de odio en particular, o si tus relaciones son tensas debido a diferencias políticas o personales. Si no te sientes capaz de hacerlo, puedes pedir a un amigo que tenga experiencia en estos asuntos que mantenga las conversaciones más difíciles por ti.

Si la dirección de tu casa está incluida en el doxeo, a ser posible, busca un nuevo lugar en el que puedas quedarte. Si no puedes salir de tu casa, invita

a tus amigos o a un grupo de seguridad local a quedarse contigo. Haz una «mochila de emergencia» (Go-Bag) con todo lo necesario si tienes que hacer las maletas e irte con poco margen de tiempo.[12]

Evaluando las amenazas

Si no sientes que corres ningún gran riesgo, especialmente si tu doxeo se compone de información de libre acceso o simplemente te lo envían directamente con la intención de ponerte nervioso, puede que te sientas bien desechándolo como una táctica de intimidación barata, bloqueando y denunciando al acosador, y pasando página. Es posible que sólo se trate de alguien intentando sacarte de quicio. Sin embargo, si el doxeo incluye información personal sensible, con detalles específicos que son difíciles de encontrar sin un buen método de espionaje, o aparece en un foro público donde la gente distribuye información con la esperanza de que otros actúen sobre ella, es posible que quieras tomar precauciones más serias. Esto es especialmente cierto si ya formas parte de un grupo (demográfico) señalado.

Cuando sepas que has sido doxeado, es importante establecer qué información podría traducirse en amenazas creíbles. A menudo, el doxeo es un precursor de un acoso más intrusivo fuera de Internet, o está relacionado con amenazas de actuar en base a la información. Esto podría significar cualquier cosa, desde llamadas telefónicas a tu familia o puesto de trabajo hasta amenazas de muerte o una llamada a los SWAT.

A veces es complicado determinar qué hace que una amenaza sea «creíble». La táctica más común de los doxeadores ordinarios es enviar mensajes extraños o intimidantes allí donde creen que pueden llegar a ti —redes sociales, correos electrónicos, familiares, etc. A menudo insinúan que tienen más información de la que en realidad poseen; es común en ellos que digan que han proporcionado esta información a las fuerzas de

[12] *NdT:* En motores de búsqueda como Google, ofrecen un servicio[13] de atención a la privacidad de petición a eliminar todo contenido que involucre una vulnerabilidad a tu intimidad, apelando al Derecho al Olvido, sin necesidad de otorgar información adicional que no sea tu nombre y correo electrónico.

[13] https://support.google.com/legal/troubleshooter/1114905

seguridad locales. Su objetivo es intimidarte para que no actúes; a menudo, la información que publican es la única que tienen.

La empresa en la que trabajas puede recibir llamadas exigiendo que te despidan. Hasta ahora, es raro que los objetivos del doxeo hayan sido atacados físicamente, pero ha pasado, y es posible que quienes te doxeen se esfuercen por hacer llegar tu información en manos de quienes no actúan de forma racional o ética. Es importante ser cauteloso, no entrar en pánico ni sumergirse en la ansiedad.

Pregúntate:

- ¿Es esta información cierta? ¿Tienen la dirección de tu casa, trabajo o familiares? ¿Conocen los lugares que sueles frecuentar? ¿De quiénes eres amigo?
- ¿Estás en riesgo de perder tu trabajo si encuentran cierta información tuya?
- ¿Sabes dónde vive el acosador? ¿Son cercanos a tu comunidad física o son meros trolls de Internet en un foro descentralizado? ¿Tienes motivos para creer que los cuerpos de policía estén interesados en esta información?
- ¿La información que se comparte proviene de fuentes locales de noticias de la derecha, poniendo tu cara frente a una multitud de extraños hostiles que ahora tienen tu información?
- ¿Tienen alguna foto tuya embarazosa o especialmente íntima?
- Existe información que te vincule a una actividad criminal que pueda provocar tu detención?

Soluciones

He aquí algunas cosas que puedes hacer en respuesta a los peligros que pueden surgir por ser doxeado:

- Crea un plan de autodefensa, contacta un grupo de defensa comunitario de tu zona.
- Informa a la gente y grupos mencionados en el doxeo—puestos de trabajo, camaradas, compañeros de piso, familia.
- Habla de tus miedos con la gente que confías.

- Contacta con la gente que ya haya pasado por este proceso para pedirles consejo.
- Planea tener un abogado disponible si te preocupa que la información sobre ti pueda ser de interés para los agentes del Estado.
- Contacta con grupos antifascistas de tu zona—puede que te ayuden a identificar a los doxeadores en caso de que haya sido publicado desde una cuenta falsa.

Mantén conversaciones con el trabajo y la familia

Esta conversación puede ser muy difícil, especialmente si tu relación con tu familia no es favorable. Ten a mano un amigo con la cabeza fría para que te ayude a mediar o te apoye después si es necesario.

Piensa en la frecuencia con la que estás dispuesto a ser vulnerable con tu familia y en las oportunidades que se te avecinan para seguir la conversación. Si es necesario hablar con la familia, pero crees que sólo tendrás una sola oportunidad, puedes ensayar con un amigo y prepararte para sus reacciones. Si tienes una relación estable, conversacional y de confianza, puedes explicarles la situación en una serie de pequeñas conversaciones, en vez de una larga sentada. Evalúa cuánto tiempo y cuánta atención vas a tener.

Siempre me ha ayudado enmarcar esto como si «tuviera un acosador» a las personas con las que no quiero tener una conversación política—eso puede ser suficiente para explicarles la gravedad del asunto y el por qué necesitas privacidad. Esto puede ser de ayuda para construir relaciones más sólidas y desmitificar este hecho tan común, a la vez que anima a otras personas que quizás no se hayan planteado que pueda ocurrirles a ellos, o a alguien cercano, a tomarse en serio la privacidad online. La mayoría de la gente responderá con miedo y simpatía, aunque a veces sugerirán, e incluso insistirán, en que llames a la policía.

No hay un enfoque exclusivo para todos. En mi caso, tuve que obligar a mi conservadora madre a prometer que no involucraría a la policía. Lo hice apelando a mi derecho a la seguridad personal y a mi autonomía como víctima de la situación, pidiéndole que respetara mis deseos y recordándole que la policía puede hacer muy poco para responder a un acoso selectivo como éste—y que lo único que conseguiría acudiendo a ellos

sería exponerme a su escrutinio, pues se me acusaba de actividad criminal. Recuerda a tus amigos y familiares que no deben reaccionar ni responder a las llamadas telefónicas, los correos electrónicos o las solicitudes de las redes sociales.

Puedes leer una guía sobre cómo discutir esto con tu empresa/compañeros de trabajo aquí.[14]

Cosas que debes recordar cuando hables con tus amigos y familiares:

- El objetivo del acusador es aislarte de tus relaciones y arruinar tu vida. No permitas que se salga con la suya. Dile a tu familia que la mejor forma de apoyarte es evitando caer en sus tácticas.
- No vendas a los anarquistas y antifascistas o afirmes que estás siendo atacado sin razón. Esto no te servirá si surgen razones—y sólo deslegitimará y pondrá en peligro a aquellos que no pueden distanciarse de la política anarquista.
- No dejes que nadie te culpe de lo que está pasando, ya sea por la política a la que te adhieres o por tu supuesta irresponsabilidad por haberte metido «en esta situación». Luchar por un mundo mejor implica desafíos. En cualquier caso, tiene el mérito de haber provocado esta respuesta por tus esfuerzos.
- Sugiere formas concretas en las que puedas ayudarles a entender la situación y a protegerse. Envíales este artículo o una lista de recursos; ofrécete a ayudarles a bloquear sus redes sociales si no tienen experiencia con la tecnología.
- Háblales de a lo que pueden prepararse—llamadas de teléfono amenazantes, correos electrónicos, quizás los vecinos reciban mensajes sobre ti. Prepáralos para el peor de los casos, pero haz hincapié en que es poco probable.
- Sé claro sobre lo que necesitas de ellos.

Vive tu vida, avanza

Respira profundamente. No te martirices. Emocionalmente esto puede ser verdaderamente inquietante y perturbador, con un toque de estrés agudo en tu vida. Es posible que haya gente que sepa cómo eres y no

[14]https://crashoverridenetwork.com/employers.pdf

tengas ni idea de quiénes son. A veces, la información de los doxeadores se convierte en una parte permanente en Internet si tu nombre es googleado; esto puede afectar a tus perspectivas de trabajo. En ocasiones, nada ocurre con la atención—pero la constante posibilidad de que alguien intente continuar donde lo dejó el último doxeador existe.

Hasta que estés seguro de que tu tiempo en el punto haya finalizado, puede que tengas que modificar algunos aspectos de tu vida. Pregúntate, «¿Qué tipo de vida quiero llevar? ¿Cómo puedo paliar mi ansiedad? ¿Hay formas de aceptar ser una figura más pública? ¿Cómo puedo volverme a sentir seguro al asumir riesgos y volver a ser activo?». Especialmente, a medida que se intensifican las tensiones políticas, puede ser importante extremar las medidas de seguridad.

He aquí algunas de las medidas que puedes emplear:

- No dejes que nadie te fotografíe, a menos que confíes en que manejará las imágenes de la manera que necesitas. Esto puede acarrear conversaciones incómodas, especialmente en eventos familiares o en situaciones laborales. Sé consciente de quién aparece en las fotos contigo; informales de que aparecer en una foto contigo puede atraer una atención no deseada. Puede ser útil ensayar las conversaciones que puedas necesitar.
- Instala cámaras de seguimiento en tu casa.
- Lleva un registro de todo el acoso que experimentas.
- Si te mudas, no actualices tu dirección. No te registres para votar, pues esto hace pública tu dirección. Intenta conservar tu antiguo carné de conducir o documento de identidad y recibe el correo en un apartado de correos. Considera cuándo utilizar tu dirección real y cuándo usar una falsa u omitir tu dirección en sitios web.
- Si es necesario, utiliza pseudónimos online y en persona. No utilices el mismo constantemente.
- Cuando vayas a acciones, y más si no te cubres la cara, presta atención de qué grupos, lugares o individuos podrían estar implicados a ser vistos o fotografiados en tus alrededores.

- Invierte tiempo en clases de defensa personal. Esto puede incluir el entrenamiento con armas, pero debería ser suficiente el entrenamiento defensivo y de desarme.
- Visita un terapeuta para trabajar cualquier trauma que hayas experimentado.
- Ayuda a tus amigos y familiares a entender la importancia de la seguridad online.
- Ten conversaciones honestas con personas fuera de tus círculos de afinidad política. Puede sorprenderte cuánta empatía pueden mostrar.

No importa la intensidad con la que tus acosadores traten de aislarte, no estás solo. Como comunidad, debemos protegernos los unos a los otros y a nuestras redes online del acoso, el encarcelamiento, la violencia política y la intimidación. Juntos, **podemos hacerlo**.

Esta guía detallada explica cómo protegerse de los acosadores en línea, por qué es importante hacerlo y qué hacer si eres víctima de «doxeo»—la publicación de tu información privada.

No Trace Project / Sin rastros, no hay caso. Una colección de herramientas para ayudar a anarquistas y rebeldes a **comprender** las capacidades del enemigo, **debilitar** los intentos de vigilancia, y por último, **accionar** sin ser atrapades.

Dependiendo de tu contexto la posesión de ciertos documentos podría ser criminalizada o atraer la atención. Ten cuidado con los fanzines que imprimas y donde los almacenes.