Lista de Defensa Doxxing

ACTIVIST CHECKLIST

Última actualización **22 de mayo de 2026** Toma unos **45 minutos para las protecciones básicas**

Esta copia se hizo el 14 de noviembre de 2026. Actualizamos nuestras guías seguido, a medida que cambian las amenazas y surgen mejores formas de protegerte. Para ver la versión más reciente, visita activistchecklist.org/es/doxxing/

Traducido automáticamente: Esta página se tradujo automáticamente. Hasta ahora solo el 12% de la página fue revisado por una persona. El resto del texto puede tener errores. Ayúdanos a revisar esta traducción[1].

El **doxxing** ocurre cuando acosadorxs recopilan y publican información personal identificable sobre alguien, con la intención de acosarlx o intimidarlx. A menudo deriva en acoso en línea y puede llevar a perder el trabajo, a consecuencias legales (hemos visto a ICE usar datos recopilados para detener personas) y, en casos raros, a daño en persona.

La información revelada puede incluir tu nombre legal completo, domicilio, lugar de trabajo, número de teléfono, correo, fotos, familiares, etc.

Por qué esto es importante: Nuestra oposición usa el doxxing y el acoso en línea porque quieren *generar miedo* para que dejemos de hacer nuestro trabajo. Mientras más medidas tomemos para defendernos de antemano, más poder tendremos en nuestras acciones. Si esperas hasta después de haber sufrido doxxing, la información ya estará allá afuera y fuera de tu control.

Cómo el doxxing se convierte en acoso y daño

Ejemplos de acoso que pueden surgir del doxxing: Una vez que tu información se ha compartido, estos son los tipos de acoso que pueden ocurrir: envío de correos/mensajes acosadores, intentos de hackear tus cuentas en línea, envío de paquetes a tu dirección, suplantarte en línea, atacar a tu empleador para dañar tu reputación o lograr que te despidan, intentos de abrir tarjetas de crédito a tu nombre, entregar tu información a ICE o a la policía para que te arresten, o intentar cualquiera de estos ataques contra tu familia o amigxs.

La mayoría de los casos de doxxing se quedan en línea. Las raras escaladas en persona han incluido vandalismo a la propiedad, atacantes que se presentan en tu casa o lugar de trabajo para acosarte, contratar un "camión de doxxing[2]" para desprestigiarte en público, swatting (llamar a un equipo SWAT contra ti) y, lo más grave, funcionarios del gobierno usando los datos recopilados para detener personas. Esto es poco probable a menos que seas una figura pública.

Vías que podría usar un atacante:

- Podrían buscar tu nombre en motores de búsqueda (como Google) o en redes sociales
- Podrían buscarte en LinkedIn o encontrar una copia de tu currículum para conocer tu lugar de trabajo, escuela e historial profesional
- Podrían usar fotos que has publicado en línea para deducir dónde vives o en qué lugares pasas tiempo
- Podrían buscarte en sitios de "people search" para obtener tu dirección a partir de tu nombre o número de teléfono
- Podrían buscar tu número de teléfono en Venmo para ver dónde pasas el tiempo según a quién le pagas y cuándo
- Podrían usar una foto tuya (obtenida en línea o tomada en una protesta) para hacer una "búsqueda inversa de imagen" y encontrar tus perfiles en línea.

Luego pueden compartir esta información públicamente de varias formas: en "sitios de doxxing" públicos (por ejemplo Canary Mission[3]), en redes sociales, o en canales semipúblicos como Telegram y foros de la dark web.

Cómo podemos protegernos a nosotrxs mismxs y a nuestra comunidad

Qué queremos proteger: Nuestra meta es que tu información personal identificable y sensible sea mucho más difícil de recopilar, empezando por lo más crítico: tu domicilio y tu lugar de trabajo.

Háganlo juntxs. Muchos grupos que hacen trabajo público abordan esta lista como una security party[4] para que todxs queden blindadxs al mismo tiempo.

Estamos en este trabajo porque tenemos un compromiso con transformar los sistemas y la cultura. Es fácil leer guías como esta y pensar "necesito esconderlo todo y no volver a salir". Ese tipo de miedo es exactamente lo que nuestra oposición espera lograr si nos amenaza lo suficiente. En lugar de eso, te animamos a usar estas medidas defensivas para empoderarte y **seguir tomando acciones audaces**.

Mientras más éxito tengas en tu trabajo, más probable es que en algún momento enfrentes algún tipo de doxxing o acoso en línea. Considéralo una señal de que vas por buen camino.

¿Estás viviendo doxxing o acoso en línea en este momento? Si es así, salta a la sección de respuesta ante el doxxing más abajo.

Protecciones básicas

TODO EL MUNDO Esta sección es para ti si estás haciendo cualquier tipo de activismo o incidencia que pueda atraer la atención de tu oposición.

Mira lo fácil que es encontrar tu dirección de casa en Google usando solo tu nombre o número de teléfono

Lo mejor que puedes hacer para entender lo importante que es proteger tu perfil público es buscarte a ti misme.

Más adelante en esta guía, harás una búsqueda manual detallada en Google. Pero por ahora, **el objetivo es simplemente ver qué información privada tuya es fácil de encontrar**.

CÓMO HACER UNA BÚSQUEDA INICIAL EN GOOGLE DE TU INFORMACIÓN PRIVADA: INTENTA ENCONTRAR TU

Busca en Google lo siguiente, reemplazando los valores de ejemplo con tu información real:

- `"555-867-5309"` (tu número de teléfono)
- `"Jamie Garcia" address` (tu nombre más la palabra "address")
- `"Jamie Garcia" phone number` (tu nombre más las palabras "phone number")
- `"Jamie Garcia" "Springfield High School"` (tu nombre más tu escuela secundaria o universidad)
- `"Jamie Garcia" employer` (tu nombre más la palabra "employer", o prueba con el nombre de tu lugar de trabajo)

Usar comillas ayuda pero no es obligatorio. Si no encuentras nada, inténtalo sin comillas.

Tu tarea: **¿Cuánto tardas en encontrar tu dirección de casa?**

Seguramente no mucho. El resto de esta guía te ayudará a eliminar mucha de esta información.

Importante Elimina tu información de los sitios de "búsqueda de personas" usando un servicio automatizado (como EasyOptOuts)

Usar una herramienta para eliminar tu información automáticamente de todos estos sitios te ahorra mucho tiempo.

DO: Regístrate en EasyOptOuts[5] ($20/año) — o en Optery Ultimate[6] ($249/año) para mayor cobertura

DO NOT: No recomendamos DeleteMe porque es menos efectivo que EasyOptOuts

Los **sitios de "búsqueda de personas"** son un tipo de "data broker". Recopilan información de registros públicos y privados para armar un "perfil" de prácticamente cualquier persona. Si alguna vez has tenido un número de teléfono, usado una tarjeta de crédito o votado, probablemente estés en alguno de estos sitios.

Pruébalo: Busca tu nombre o número de teléfono en este sitio[7] (lo usamos como ejemplo porque muestra los resultados al instante, sin pedirte que te registres). A la mayoría de la gente le sorprende cuánta información está disponible fácilmente. Otros sitios importantes de esta categoría son Whitepages, Spokeo, BeenVerified, y un número creciente de herramientas de búsqueda con IA.

Por qué pagar por servicios de eliminación automática: Puedes hacer este proceso de "exclusión" manualmente, pero toma una cantidad enorme de tiempo, y tienes que repetirlo cada pocos meses cuando los sitios de corredores de datos cambian. Es ridículo que tengamos que pagar para proteger nuestra privacidad, pero nos ahorra mucho tiempo para enfocarnos en nuestra organización.

¿Qué herramienta de eliminación automática debería usar?

- **EasyOptOuts[5] (recomendado)** - $20/año - Es de los más efectivos[8] y el más barato.
- **Optery Ultimate[6]** - $250/año - Un poco más efectivo si puedes pagar la inversión adicional. Pueden tomar una copia de tu identificación (con el número de ID borrado) y excluirte de los sitios que requieren una identificación.
- **¿Y qué hay de DeleteMe? -** Es la opción más conocida, pero solo fue 27% efectiva eliminando perfiles, comparada con EasyOptOuts (65%) y Optery Ultimate (68%). (Fuente[9]).

CÓMO ELIMINAR TU INFORMACIÓN DE LOS SITIOS DE "BÚSQUEDA DE PERSONAS" USANDO EASYOPTOUTS

Tiempo requerido: 5–15 minutos

1. **Regístrate en EasyOptOuts**[5] ($20/año)
2. **Ingresa tu información personal:** Sigue las indicaciones. Lo más importante es incluir tu información **actual** (dirección, teléfono, correo). Si no logras encontrar todas tus direcciones anteriores, no pasa nada.

   > **Advertencia:** NO ingreses **alias** ni **números de teléfonos desechables** que uses exclusivamente para el activismo y que ya estén completamente separados de tu identidad real. No querrías que queden vinculados dentro de este sistema.

3. Continúa con el siguiente punto de la lista para hacer **exclusiones manuales** en los sitios que EasyOptOuts no puede manejar.
4. Considera pedirle a cualquier persona que viva en tu casa que también se registre. Si alguien descubre que viven juntes, podría buscar a esa persona con la misma facilidad y luego atacarte a ti.

Tiempos: Las primeras eliminaciones pueden tardar unos días en completarse, y a veces hasta un par de meses para ciertos sitios.

Para tu información: No recibimos comisiones por ninguno de los servicios pagos a los que enlazamos. Los recomendamos porque son los más efectivos que hemos encontrado.

Privacidad de EasyOptOuts: A algunas personas les preocupa ingresar toda su información en un sitio así. Aunque ningún sitio está libre de filtraciones de datos, confiamos en este sitio por su historial y reputación. Y la información es necesaria para hacer las eliminaciones.

Herramienta alternativa: Kanary[10] es una app gratuita que busca tu información personal en Google y te guía para eliminarla manualmente. Aun así requiere mucho tiempo y es probable que la gente la abandone antes de terminar todas las eliminaciones.

- [ ] Importante **Date de baja manualmente de los sitios de "búsqueda de personas" que no se cubren automáticamente**

  Incluso las herramientas más efectivas para eliminarte de sitios de "búsqueda de personas" solo cubren el 70% de los sitios.

Algunos de estos sitios hacen muy difícil eliminar un perfil, así que servicios como EasyOptOuts no pueden hacerlo por ti. Por lo general, te piden recibir un correo para confirmar que tú eres quien está eliminando el perfil.

CÓMO ELIMINARTE MANUALMENTE DE LOS SITIOS DE BÚSQUEDA DE PERSONAS DE ALTO RIESGO

Empieza por darte de baja manualmente de los sitios de mayor riesgo:

1. **Date de baja de People Connect (Intelius)**[11] - Son dueños de muchos sitios de búsqueda de personas, así que una sola baja sirve para mucho. Llena el "suppression form" (formulario de supresión). Te pedirán verificar tu correo o teléfono.
   - Si el sitio te pide verificar un número de teléfono o correo al que no tienes acceso, llama a su soporte técnico al (877) 564-3253 y pide que supriman tu "personal information" (información personal). Por nuestra experiencia, llamar es mucho más efectivo que enviarles correos.
2. **Búscate en National Public Data**[12]**.** Si encuentras un resultado, baja hasta el final de la página y haz clic en Do Not Sell My Info para darte de baja[13].

Hay otros sitios que solo encontrarás buscando tu información manualmente en Google (lo explicamos en un punto posterior de la checklist).

Totalmente manual: Si quieres hacer todas las bajas a mano, puedes usar la Big Ass Data Broker Opt-Out List[14] de Yael Grauer. Servicios como EasyOptOuts se encargan de la mayoría por ti, pero no de todos. Puedes usar esta lista para hacer el proceso manualmente sin costo, o para revisar cada base de datos a mano y ver qué se te pasó.

Excluye tus datos de los sitios de "búsqueda facial"

Protégete para que una foto tuya no se use para descubrir tu identidad.

Puedes protegerte excluyendo tus datos de los sitios de "búsqueda inversa de fotos". Esto hace más difícil que alguien use tu foto de perfil en línea para averiguar tu nombre legal, lo cual podría llevarles a encontrarte en los sitios de búsqueda de personas mencionados arriba.

CÓMO ELIMINARTE DE LOS SITIOS DE "BÚSQUEDA FACIAL"

Cada uno de estos sitios (irónicamente) te pedirá que subas una foto de tu rostro. Es un mal necesario si quieres que te eliminen. Tienes que decidir si el riesgo de darles más datos vale la pena para lograr la exclusión.

> **Nota sobre subir tu identificación oficial**: Algunos de estos sitios son terribles y te piden subir una foto de tu identificación oficial o pasaporte con la información sensible oculta. Lo más fácil es poner cinta adhesiva sobre todo lo que aparece en tu identificación, excepto tu nombre y foto, y luego tomar la foto.

Sitios de los que excluirte:

1. Excluirse de Clearview.ai[15] - Solo requiere una foto, no una identificación oficial. Lamentablemente, la exclusión solo es posible en estados que han aprobado leyes de privacidad. ***Clearview lo usan principalmente las agencias policiales, así que es importante excluirte.***
2. Excluirse de PimEyes[16] - Requiere una foto de tu identificación oficial. (¡Tapa tu número de identificación!)
3. Excluirse de FaceCheck.ID[17] - En lugar de subir una identificación oficial, puedes subir una selfie en la que toques tu barbilla con dos dedos. Además, debes seleccionar manualmente las fotos que quieres que eliminen.

Activa las notificaciones de "Resultados sobre ti" de Google

Esto te ayuda a estar al tanto de las páginas que tienen tu información personal.

Google ofrece Resultados sobre ti[18] como una herramienta para que sepas cuándo se comparte tu información privada en línea. No es lo más útil para eliminar esos resultados, pero te ayuda a saber cuándo necesitas buscar formas manuales de quitar la información.

CÓMO ACTIVAR RESULTADOS SOBRE TI DE GOOGLE

1. **Activa "Resultados sobre ti" de Google**[19]: Ingresa tu nombre completo (y cualquier otro nombre que uses), direcciones, números de teléfono y correos electrónicos.

   > **Advertencia:** NO ingreses **alias** ni **números de burner phone** que uses exclusivamente para activismo y que ya estén totalmente separados de tu identidad real. No querrías que eso quedara vinculado dentro de los sistemas de Google.

2. **Espera** a que se complete el escaneo inicial (unas pocas horas)
3. **Revisa los resultados y busca formas de eliminarlos:**
   1. Usar el botón de "solicitar eliminación" dentro de la herramienta de Google normalmente no sirve de mucho por dos razones: 1) Google rechazará la mayoría de las solicitudes a menos que sean de un sitio de "búsqueda de personas" o de doxxing intencional. Y 2) la información original sigue ahí afuera aunque Google la quite. La gente puede encontrarla en otros motores de búsqueda o directamente en el sitio original.
   2. En vez de eso, conviene que intentes contactar a quien administra el sitio para que elimine la información. En los sitios web, esto significa buscar un formulario de contacto o correo y decirles cuál es la página que tiene la información que pides que eliminen. En redes sociales, esto puede significar eliminar una publicación que hiciste o pedirle a quien la publicó que la quite.
   3. Haz clic en "marcar como revisado" mientras vas resolviendo cada caso.
4. **Envía una "solicitud de eliminación" a Google:** Usa este formulario de solicitud de eliminación[20] para pedirle a Google que elimine resultados de búsqueda que contengan tu información personal u otro contenido de doxxing. Esto es distinto a la función de "Resultados sobre mí" de Google.
5. **Pendiente de los correos de notificación** sobre nuevos resultados a medida que aparezcan. Normalmente verás más durante las primeras dos semanas después de registrarte.

Privacidad: Requiere una cuenta de Google. Aquí hay un trade-off: le estás dando a Google identificadores adicionales como tus otros nombres, números de teléfono y direcciones, que quedarán registrados y vinculados a tu cuenta. Normalmente vale la pena, porque Google ya tiene casi toda esta información sobre ti, y a cambio te avisa cuando tu dirección u otra info privada aparece en algún lugar nuevo de la web.

Blinda la configuración de privacidad de tus cuentas de redes sociales

La mayoría compartimos mucha más información sobre nosotres en redes sociales antes de empezar a preocuparnos por proteger nuestra privacidad.

Blindar nuestros perfiles de redes sociales puede tomar bastante tiempo.

Cosas que tal vez quieras proteger: tu ubicación, tu correo electrónico (puede usarse para buscarte aunque esté oculto), tu lista de amistades, tu lugar de trabajo, tu fecha de nacimiento completa (puede usarse para acceder a otras cuentas como la del banco) y fotos o publicaciones que muestren dónde pasas tiempo con más frecuencia.

Ser visible y público vs. privado: algunas personas tienen perfiles públicos a propósito, con seguidores que quieren mantener porque los usan para su activismo y organización. Por ejemplo, pueden elegir mantener sus perfiles accesibles, mientras que otras prefieren ocultarlo para que solo sus amistades puedan verlo.

OPCIÓN 1: CÓMO BLINDAR LA CONFIGURACIÓN DE PRIVACIDAD DE TUS REDES SOCIALES CON BLOCK PARTY

Aunque puedes hacerlo manualmente (mira más abajo), te recomendamos usar Block Party[21] porque te guía por las configuraciones de privacidad que debes cambiar. Te ayuda a blindar Facebook, LinkedIn, Instagram, X/Twitter, TikTok, Snapchat, Reddit, Strava, Venmo, Google, reseñas de Google Maps, YouTube y Bluesky. La versión gratuita es útil, y ya revisamos su política de privacidad: en general confiamos en quienes la crearon.

1. **Instala la extensión Block Party**[22] (gratis) en tu navegador. (¡Este es un buen momento para instalar Brave[23] si aún no lo has hecho!) Sigue las instrucciones de instalación.
2. **Presiona "Start Scan"** y selecciona las redes sociales que usas. Déjalo correr unos minutos mientras revisa toda tu configuración.
3. **Junto a cada sitio, haz clic en "To Do"** para ver los cambios recomendados. Puedes empezar a hacerlos manualmente o dejar que Block Party automatice muchos de ellos.
4. **Puedes automatizar muchos de los cambios:** Block Party hará entre el 50% y el 70% de los cambios de configuración por ti automáticamente. Esto requiere una prueba gratuita de 7 días o una cuenta paga ($50 al año si usas el código promocional JOINTHEPARTY; no recibimos ninguna comisión).
5. **Haz los cambios manuales restantes:** sigue las listas de "To Do" de cada sitio que no se pueda automatizar.
6. Por último, piensa en qué otras redes sociales usas que tal vez no estén cubiertas por Block Party: Cash App, Venmo (si no está ya cubierto), Partiful, Nextdoor, AllTrails, Strava, Pinterest, Goodreads, MapMyRun, apps de citas, etc.

Si quieres borrar tus publicaciones viejas de X/Twitter o migrar a Bluesky, prueba Cyd[24].

OPCIÓN 2: CÓMO BLINDAR MANUALMENTE LA CONFIGURACIÓN DE PRIVACIDAD DE TUS REDES SOCIALES

Si no quieres usar Block Party, puedes seguir estos pasos con cada una de tus cuentas principales de redes sociales.

Sitios a los que tal vez quieras dar prioridad (aproximadamente por nivel de riesgo):

- Facebook
- LinkedIn
- Venmo
- Cash App
- Reseñas de Google Maps
- Yelp
- Strava
- All Trails
- Instagram
- X/Twitter *(para borrar tus publicaciones viejas, prueba Cyd[24].)*
- Bluesky
- YouTube
- TikTok
- Snapchat
- Reddit
- Partiful
- Nextdoor

Pasos para cada sitio:

1. **Considera borrar este perfil** si ya no lo necesitas. Muchos sitios (Facebook, Instagram, Google) te permiten descargar una copia de tus datos primero para que no pierdas fotos ni mensajes. Si lo borras, ya terminaste. Si no, sigue adelante.
    - **¿Solo necesitas Facebook Marketplace?** Considera crear una cuenta falsa aparte de Facebook para usar Marketplace, y luego elimina la principal.
2. **Busca la pantalla de configuración de privacidad** y cambia todos los ajustes para que sean lo más privados posible.
3. **Quita tu ciudad**
4. **Oculta tu lista de amistades**
5. **Depura tus seguidores/contactos.** Quita a las personas que no tengan al menos una o dos amistades en común contigo, sobre todo si en realidad no las conoces. Incluso en un perfil "privado", cualquier persona que hayas aceptado como seguidor puede ver tus publicaciones y tomarles captura de pantalla.
6. **Borra publicaciones y fotos viejas** que revelen información detallada sobre dónde vives, dónde pasas tiempo y con quién.

Considera usar Digital Footprint Check[25] con los nombres de usuario que sueles usar, para ver dónde podrías tener perfiles que olvidaste.

Usa una máscara cuando te encuentres con la policía o adversarios de derecha

Esto te ayuda a protegerte si alguien malintencionado intenta usar tu cara para descubrir tu identidad

La policía e ICE usan reconocimiento facial contra disidentes[26].

Los adversarios de derecha suelen fotografiar a manifestantes para hacer búsquedas inversas de imágenes e identificar a quienes participan; algunos mantienen bases de datos como Canary Mission[27] con perfiles de activistas. Ocultar parte o toda tu cara hace esto más difícil.

Una máscara KN95 puede ayudarte a evitar las herramientas de reconocimiento facial. No es perfecta (algunas herramientas solo necesitan tus ojos), pero ayuda bastante.

Otros rasgos identificativos también importan. Cubrirte la cara no basta si otras partes de ti son fáciles de reconocer. Quienes nos vigilan suelen identificar a manifestantes enmascarades por sus tatuajes llamativos, color o estilo de pelo, complexión, tono de piel y ropa, sobre todo cuando varios de estos se combinan. Considera cubrir tatuajes visibles con mangas largas, usar gorra o capucha, y cambiar tu ropa de protesta si quieres que sea más difícil rastrearte entre acciones.

> Como con otros puntos de esta lista, la privacidad y la visibilidad pueden entrar en tensión: algunas personas prefieren minimizar el riesgo cubriéndose la cara y los ojos, mientras que otras prefieren mostrar la cara completa para generar confianza y transmitir emociones de forma más directa.

Nota legal: algunas ciudades han aprobado leyes anti-máscara que prohíben usar máscara. Quizá quieras revisar las ordenanzas locales de tu ciudad.

Completa nuestra lista de Conceptos básicos de seguridad digital

Esta guía cubre otros pasos importantes para protegerte del doxxing, como contraseñas, permisos de ubicación en apps y actualizaciones de software.

Si te preocupa el doxxing, es buena idea completar los pasos de nuestra lista de Conceptos básicos de seguridad digital →[23]

Muchos de estos pasos te protegerán si alguien intenta acceder a tus cuentas o dispositivos cuando eres blanco de doxxing.

Estos puntos de la lista de Conceptos básicos son especialmente importantes:

- **Desactiva el rastreo de ubicación** en la mayoría de las apps
- **Instala las últimas actualizaciones de software** en tu computadora, teléfono y apps
- Usa un **gestor de contraseñas**
- **Cambia tus contraseñas actuales** si son débiles o las reutilizas en varios sitios.
- Activa la **autenticación de dos factores** en tus cuentas importantes
- No hagas clic en **enlaces sospechosos**

No uses tu nombre real ni tu foto en tu perfil de Signal

Te ayuda a protegerte de los policías o atacantes que quieren desanonimizarte. Es muy útil si estás en grupos de Signal sin verificar.

Mucho del trabajo de organización comunitaria pasa en grupos de Signal sin verificar, donde no sabes cuánto puedes confiar en cada quien. Estos grupos pueden ser infiltrados por adversarios de derecha[28] y los policías[29].

Usar un nombre falso evita que alguien encuentre tu identidad real con una búsqueda en Google.

Usar una foto que no sea tu cara evita que alguien encuentre tus perfiles en redes sociales por coincidencia de imagen o reconocimiento facial.

Ambos pasos te ayudan a defenderte del doxxing[30] y del acoso en línea.

CÓMO CAMBIAR TU PERFIL

1. **Cambia el nombre que muestra tu perfil:** Abre Signal → Toca tu foto de perfil → **Ajustes** → Toca tu nombre/ícono cerca de la parte superior → Toca la primera opción con la silueta de una persona → Edita el nombre que muestra tu perfil
2. **Cambia tu foto de perfil:** Abre Signal → Toca tu foto de perfil → **Ajustes** → Toca tu nombre/ícono cerca de la parte superior → **Editar foto** → sube una foto genérica que hayas encontrado en internet y que no tenga relación con tu identidad/preferencias/intereses/ubicación.

Lo mismo aplica con aún más fuerza en redes sociales. Si tu perfil de Instagram, Facebook o LinkedIn muestra tu nombre real completo junto con una foto clara de tu cara, quienes te ataquen pueden identificarte fácilmente aunque el resto de tu perfil sea privado. Mira Asegura tus redes sociales para más info.

Recuérdales a las personas de tus grupos que hagan esto también. La seguridad es un trabajo de equipo.

Protecciones reforzadas

AMENAZA MEDIA Esta sección es para ti si tienes un rol visible relacionado con tu disidencia política.

Configura Signal para que tu número de teléfono no sea localizable

Aunque tu número de teléfono no es visible en Signal por defecto, la gente todavía puede escribir tu número y encontrarte. Si estás en riesgo de acoso, tal vez prefieras compartir solo tu nombre de usuario de Signal[31] con la gente.

CÓMO HACER QUE TU NÚMERO DE TELÉFONO NO SEA LOCALIZABLE EN SIGNAL

1. **Si quieres cambiar tu nombre de usuario:** Abre Signal → Toca tu foto de perfil → **Ajustes** → Toca tu nombre/ícono cerca de la parte superior → Toca el símbolo **@** → **Editar nombre de usuario** → elige un nombre de usuario **completamente ajeno** a tu identidad, o a cualquier nombre de usuario que hayas usado antes en otros lugares. Debe terminar en al menos 2 números.
2. **Oculta tu número de teléfono:** Abre Signal → Toca tu foto de perfil → **Ajustes** → **Privacidad** → **Número de teléfono** → En **Quién puede ver mi número** → Selecciona **Nadie**.
3. **Haz que tu número de teléfono no sea localizable:** Abre Signal → Toca tu foto de perfil → **Ajustes** → **Privacidad** → **Número de teléfono** → En **Quién puede encontrarme por número** → Selecciona **Nadie**.
4. Dile a la gente tu nombre de usuario en vez de tu número de teléfono cuando quieras conectar con ellos en Signal.

Consigue un número de teléfono alternativo en lugar de compartir tu número principal públicamente

Tu número de teléfono puede ser una forma rápida para que la gente encuentre tu dirección de casa usando sitios de "búsqueda de personas".

DO: Usa Google Voice[32] (gratis, menos privado) o MySudo[33] ($2/mes, más privado)

DO NOT: Compartir tu número de teléfono públicamente en línea o en espacios grandes sin filtrar

Compartir tu número de teléfono principal públicamente no solo te pone en riesgo de llamadas/mensajes de acoso, sino que si alguno de los sitios de "búsqueda de personas" no te ha eliminado, alguien podría usar tu número de teléfono para encontrar tu dirección de casa.

CÓMO CONFIGURAR NÚMEROS DE TELÉFONO ALTERNATIVOS

- **Consigue un número de teléfono alternativo** si necesitas compartir un número de teléfono públicamente.
  - Google Voice[32] es gratis, pero Google es el primer lugar al que la chota irá a pedir información mediante una orden judicial, así que es la opción menos privada.
  - MySudo[33] cuesta $2 al mes por 100 mensajes de texto y 30 minutos de llamadas.
  - Sideline[34] ($15/mes) o Line2[35] ($10/mes) si necesitas mensajes de texto/llamadas ilimitadas
- **Cuando necesites que la gente te contacte en Signal, diles tu nombre de usuario de Signal**[31] en lugar de tu número de teléfono. (Por supuesto, usa Signal[36] siempre que sea posible, especialmente cuando estés organizando. Y asegúrate de activar los mensajes que desaparecen por defecto en la configuración.)

Pídele a las personas con quienes vives que borren su información privada de los sitios de "búsqueda de personas"

Todas las personas en tu casa necesitan proteger su información si quieres que tu dirección sea privada.

Una de nuestras metas principales es proteger tu dirección de casa de personas malintencionadas.

Alguien con motivación para atacarte podría averiguar con quién vives a través de publicaciones en redes sociales, listas de amistades o sitios de árboles genealógicos. Si tú ya te quitaste de los sitios de búsqueda de personas pero tus compañeres de casa o familiares no lo han hecho, esa persona todavía podría encontrar tu dirección.

Los familiares que comparten tu apellido son un vínculo especialmente fuerte, ya que quienes te buscan pueden saltar de cualquiera de ellos directo a la dirección que comparten contigo en los sitios de "búsqueda de personas".

CÓMO APOYAR A LAS PERSONAS CON QUIENES VIVES PARA QUE BORREN SU INFORMACIÓN PRIVADA

1. **Pídele a cada persona** con quien vives que borre su información privada de los sitios de "búsqueda de personas". Texto/mensaje de ejemplo:

   > Estoy trabajando para borrar nuestra dirección y mi otra información privada del internet, para que estemos más protegides. ¿Puedes tomarte unos minutos para hacer los primeros dos puntos de esta lista, para que nuestra dirección no sea fácil de encontrar en línea?: https://activistchecklist.org/doxxing[37]> Con gusto me siento contigo a hacerlo juntes si tienes tiempo esta semana.

2. Si te sirve, puedes buscar tu dirección en Google y encontrar páginas específicas donde su nombre aparece junto con la dirección. También puedes enviarles el enlace de esta página para ayudarles a entender por qué es importante. A la mayoría de la gente le sorprende descubrir lo fácil que es encontrar esta información en línea.
3. **Pon un recordatorio** para volver a hablar con ellas en una semana más o menos y ver si necesitan apoyo.

También puedes hacerle la misma petición a personas que vivieron contigo en tu dirección actual, ya que su dirección anterior sigue apareciendo en los sitios de "búsqueda de personas".

Haz una búsqueda manual en Google de tu información privada

Siempre habrá resultados que tendrás que encontrar y eliminar manualmente.

Si solo confías en herramientas automáticas para eliminar datos como EasyOptOuts, lo más probable es que sigan apareciendo muchos resultados con tu información privada.

Lo que más nos importa es eliminar tu dirección actual y, en segundo lugar, tu número de teléfono. Tu correo puede ser público y generar acoso, pero es más fácil de manejar.

La app Kanary[10] (versión gratuita) puede ayudarte con parte de este trabajo de búsqueda.

CÓMO ENCONTRAR Y ELIMINAR TU INFORMACIÓN PERSONAL EN GOOGLE

1. **Haz búsquedas separadas en Google con tu información.** Usa comillas en tu búsqueda para obtener más precisión. Revisa las primeras 2 o 3 páginas de Google en cada búsqueda (no uses Brave Search ni otros buscadores de privacidad para esta tarea).
   - **Dirección entre comillas:** `"742 Evergreen Terrace, Springfield"` o incluso solo `"742 Evergreen Tr"`, aunque eso puede arrojar demasiados resultados que no sean de tu ciudad.
   - **Número de teléfono entre comillas:** `"555-867-5309"` o `"5558675309"` o `"(555) 867-5309"`
   - **Nombre completo más ciudad (cada uno entre comillas separadas):** `"Jamie Garcia" "Springfield"`
   - **Solo tu nombre completo entre comillas:** `"Jamie Garcia"` (arrojará muchos resultados que tal vez no sean tuyos)
2. **Haz una lista** de lo que encuentres que incluya tu información privada sensible. Prioriza los sitios que muestren tu dirección o número de teléfono.
3. **Haz un plan para eliminar cada uno.**
   - Si es un sitio de "búsqueda de personas", busca un formulario para "no vender mi información" o para hacer opt out.
   - Si es una red social, quien lo publicó tiene que eliminarlo. O puedes intentar darle a "reportar contenido" si no quieren eliminarlo.
   - Si es otro sitio, busca un formulario de contacto y pídeles que lo eliminen porque te preocupa ser blanco de ataques en línea. La mayoría de los sitios están dispuestos a ayudar.
   - **Pide a los buscadores que eliminen el resultado.** Para casos de acoso, doxxing u otro contenido dañino, puedes enviar una solicitud de eliminación directamente a Google (formulario[20]) y a Bing (formulario[38]). Las tasas de éxito varían, pero vale la pena intentarlo para los resultados más dañinos.
4. **Pon un recordatorio para volver a revisar.** Vuelve a checar después de una semana. Si ninguno de estos sitios te respondió, intenta dar seguimiento.
5. **Configura Google Alerts**[39] para cada búsqueda de arriba, así te avisan cuando aparezcan cosas nuevas. (La función "Resultados sobre ti" de Google está bien, pero definitivamente se le escapan cosas.)
6. **Actualiza los resultados de Google.** Si lograste que eliminaran un listado en el sitio original, pero sigue apareciendo en los resultados de Google, puedes pedir que actualicen el contenido[40].
7. **Prueba también otros buscadores.** Cada buscador muestra resultados distintos, y quien te ataque no se limita a Google. Haz las mismas búsquedas en Bing y DuckDuckGo para ver qué más aparece.

☐ Congela tus reportes de crédito

Te protege de que alguien intente abrir tarjetas de crédito a tu nombre.

Alguien con malas intenciones podría intentar abrir tarjetas de crédito a tu nombre, lo cual puede dañar tu puntaje crediticio y causarte problemas financieros a largo plazo.

Congelar tu reporte de crédito impide que cualquier persona abra tarjetas o préstamos a tu nombre. Puedes descongelarlo temporalmente cuando lo necesites.

CÓMO CONGELAR TU REPORTE DE CRÉDITO

Tienes que poner un "congelamiento" manualmente en **las tres** agencias de crédito:

- **Equifax**[41]
- **Experian**[42]
- **TransUnion**[43]

Esto siempre es gratis. No aceptes ninguna oferta de pago que te ofrezcan.

Vas a tener que acordarte de levantar el congelamiento temporalmente cuando necesites que consulten tu reporte de crédito para abrir una cuenta nueva en el futuro.

Difumina tu casa en Google Maps y Apple Maps

Esto hace más difícil que alguien con malas intenciones conozca la distribución de tu casa/jardín.

Si alguien con malas intenciones consigue tu dirección, puede intentar encontrar tu casa en Google Maps si tiene la intención de acosarte o hacerte daño en persona. O podría llegar a saber cosas como qué tipo de auto está estacionado en tu entrada.

CÓMO DIFUMINAR TU CASA EN SITIOS DE MAPAS

Nota: No puedes deshacer un difuminado una vez que lo solicitas. Para la mayoría de la gente, hay muy poco beneficio en tener tu casa visible en Street View.

Difumina tu casa en Google Maps (detalles[44]):

1. Encuentra tu hogar en Google Maps[45].
2. Abre la imagen de Street View que quieres difuminar.
3. En la parte inferior derecha, haz clic en "Reportar un problema" y completa el formulario indicando que quieres difuminar tu casa por razones de privacidad.

Difumina tu casa en Apple Maps:

1. Envía un correo electrónico a mapsimagecollection@apple.com. Incluye la dirección de tu hogar y explica que quieres que sea difuminada por razones de privacidad.

Quita tu casa de los sitios de bienes raíces (Zillow, Redfin, etc.)

Ocultar las fotos del interior de tu casa ayuda a mantener a todes más seguros.

Zillow, Redfin, Realtor.com y otros suelen mostrar no solo el exterior de tu casa (lo cual ya implica cierto riesgo), sino también un plano detallado del interior. Esto puede darle a la oposición información que les ayude a acosarte o hacerte daño.

Puedes protegerte pidiendo que quiten las imágenes de tu dirección.

CÓMO QUITAR LAS IMÁGENES DE TU CASA DE LOS SITIOS DE BIENES RAÍCES

Si no eres dueñe de la casa, quizás tengas que pedirle a tu arrendador que haga estas eliminaciones, ya que requieren una cuenta en cada sitio. Tienen que "reclamar" la casa en cada sitio de bienes raíces.

También puedes buscar primero en el sitio para ver qué tan detalladas son las fotos y si quieres que las quiten.

1. Quitar de Zillow[46]
2. Quitar de Redfin[47]
3. **Realtor.com**: Inicia sesión → **Claim Home** → **Edit Photos**
4. Pídele a tu agente inmobiliario que quite las fotos del MLS para que desaparezcan de los demás sitios.

☐ Activa el Modo Aislamiento (iPhone) o Protección Avanzada (Google y Android)

El spyware es un tipo de ataque avanzado que aprovecha vulnerabilidades sofisticadas en nuestros dispositivos. En respuesta, Apple y Google han creado un modo de seguridad avanzado que ofrece mayor protección contra el spyware.

En los iPhone se llama **Modo Aislamiento**[48] y en Android se llama **Programa de Protección Avanzada**[49]. (También puedes activar el Programa de Protección Avanzada solo en tu cuenta de Google aunque no tengas un teléfono Android.)

No tenemos reportes de nadie que se haya infectado con spyware teniendo activado el Modo Aislamiento de Apple. La Protección Avanzada de Android es más reciente y todavía no se ha podido comprobar qué tan efectiva es.

> **Compromisos de uso:** Ambas funciones implican sacrificar algunas funcionalidades. Mira la lista completa de compromisos[50]. Si te topas con problemas que no te funcionan, siempre puedes desactivar la función después.

CÓMO ACTIVAR EL MODO AISLAMIENTO EN IPHONE

IPHONE

Ajustes → **Privacidad y seguridad** → **Modo Aislamiento** → **Activar**

Esta función está disponible para iOS 16 en adelante.

CÓMO ACTIVAR LA PROTECCIÓN AVANZADA EN ANDROID

ANDROID

Ajustes → **Seguridad y privacidad** → en **Otros ajustes** toca **Protección Avanzada**

Nota: La ubicación de este ajuste puede variar entre dispositivos Android, así que te recomendamos buscar 'Protección Avanzada' en la barra de búsqueda de Ajustes.

Esta función está disponible para Android 16 en adelante.

☐ Activa el PIN de Signal y el bloqueo de registro

Te protege de ataques avanzados en los que alguien "roba" tu número de teléfono y lo registra en Signal

Si alguien con mucho interés en atacarte logra averiguar tu número de teléfono, puede intentar robártelo con algo llamado " SIM Swapping" o llamando a tu compañía telefónica para pedir una "portabilidad" de tu número a otra compañía. Luego podrían usar tu número de teléfono para registrar una cuenta de Signal y empezar a recibir mensajes dirigidos a ti.

Estos son ataques avanzados que no le pasan a la mayoría de la gente. Aun así, es fácil proteger tu cuenta de Signal.

Puedes protegerte activando el **bloqueo de registro** en Signal. Evita que alguien secuestre tu cuenta, incluso si te roban el número de teléfono. Nadie podrá registrar una nueva cuenta de Signal con tu número hasta que tu cuenta haya estado inactiva por 7 días.

Si olvidas tu PIN, tendrás que esperar 7 días antes de poder crear una cuenta nueva (y tus contactos no se recuperarán). Más sobre los PIN y el bloqueo de registro[51].

CÓMO ACTIVAR EL PIN DE SIGNAL Y EL BLOQUEO DE REGISTRO

Activa el bloqueo de registro: Abre Signal → Toca tu foto de perfil → **Ajustes** → **Cuenta** → Activa **Bloqueo de registro**

Mejora tu PIN: Tuviste que configurar un PIN de Signal durante la instalación. Si no lo recuerdas o quieres usar un PIN más fuerte, así es como puedes hacerlo:

1. **Genera un PIN fuerte:** Para máxima seguridad, usa un PIN de 8 o 10 dígitos y asegúrate de que sea generado por computadora. Aquí tienes un generador de PIN aleatorios[52] que puedes usar.
2. **Configura un PIN de Signal:** Abre Signal → Toca tu foto de perfil → **Ajustes** → **Cuenta** → **Crear/Cambiar PIN** (Si aún no sabes cuál es tu PIN).
3. **Guarda tu PIN o activa los recordatorios de PIN:** Si tienes un gestor de contraseñas[23] que usas con regularidad, guarda tu PIN ahí. Si crees que podrías olvidar dónde guardaste tu PIN, deja activados los "recordatorios de PIN".

Protecciones para perfiles públicos

AMENAZA ALTA Esta sección es para ti si podrías terminar recibiendo mucha atención mediática por tu disidencia o si tus adversarios cuentan con muchos recursos.

☐ Invierte en servicios avanzados de eliminación de datos (ej: Optery Ultimate)

Si estás en un riesgo muy alto de ser atacada por tu actividad política, vas a querer asegurarte de haber hecho un trabajo a fondo eliminando tus datos en línea.

Empieza actualizando tu herramienta automatizada de eliminación de datos de EasyOptOuts a algo como Optery Ultimate[6] ($250/año). Es una de las herramientas automatizadas de cancelación de suscripción más completas. También puedes considerar el plan Kanary Pro[10] ($10/mes) para una cobertura adicional.

Dependiendo de tu nivel de riesgo, puede que quieras invertir en un servicio de alta gama que pueda hacer una limpieza exhaustiva de tus datos.

Servicios de limpieza de datos y respuesta al doxxing alineados con el activismo:

- Brightlines[53]
- Convocation Research & Design[54]

También puedes echarle un vistazo a la Línea de Ayuda de Access Now[55], que generalmente es gratuita, pero mucho más lenta y menos exhaustiva.

Haz una limpieza avanzada de redes sociales y blinda todo

Los pasos básicos para blindar tus redes sociales son un buen comienzo. Si corres un alto riesgo de ser blanco de ataques, deberías hacer una limpieza más a fondo.

CÓMO HACER UNA LIMPIEZA Y BLINDAJE DETALLADO DE TUS REDES SOCIALES

1. Haz una lista de todos los sitios donde tienes o tuviste un perfil, incluso los que no usas desde hace años. Piensa más allá de las grandes plataformas: las apps de citas, de ejercicio, de pagos, los sitios de reseñas y los foros viejos también cuentan.
2. Busca tus nombres de usuario más comunes en Digital Footprint Checker[25] y en Instant Username[56] para encontrar perfiles que hayas olvidado. Agrégalos a tu lista.
3. Revisa tu lista y sigue estos pasos en cada sitio:
   - Elimina el perfil si ya no lo necesitas
   - Cambia tu nombre visible
   - Cambia tu nombre de usuario
   - Quita tu foto de perfil
   - Quita tu ubicación de la biografía
   - Oculta publicaciones y fotos que puedan revelar tu ubicación
   - Oculta tu lista de amistades
   - Cambia tu dirección de correo electrónico (puedes usar DuckDuckGo Email Protection[57] o el "truco del signo +" de Gmail[58]).
   - Ajusta tu configuración de privacidad.
4. Esto puede tomar varias horas. Marca cada sitio cuando termines para que puedas retomar donde te quedaste.

Consejo: puedes usar este generador de identidades[59] si necesitas un nombre visible, un nombre de usuario o una foto de perfil al azar.

Abre un PO box para dejar de dar tu dirección de casa

DO: Abre un PO box[60] o usa un servicio de reenvío/escaneo de correo como iPostal1[61]

DO NOT: Seguir dando tu dirección de casa a la gente

Quizás quieras dejar de dar tu dirección real cuando te registras en servicios, recibes paquetes, etc.

Opciones:

- **PO box con USPS**[60]: la desventaja principal es que FedEx y UPS no entregan en un PO box.
- **UPS Mailbox**[62]: más caro, pero recibe correo de USPS y FedEx, y además te da más privacidad.
- **iPostal1**[61]: te ofrece escaneo de correo + recogida física, y también acepta entregas de todos los servicios de envío (incluidos FedEx y UPS) que no siempre entregan en PO boxes. Tiene un riesgo de privacidad si alguna vez hackean sus servicios, o si reciben una orden judicial para entregar tus datos.

Nota: UPS Mailbox y cualquier servicio de "buzón virtual" como iPostal1 te van a pedir una identificación oficial y que firmes un formulario (USPS Form 1583) que se envía a USPS.

☐ Usa una identidad única para cada cuenta en línea que crees (nombre, correo electrónico, nombre de usuario, número de teléfono)

En lugar de registrarte con tu nombre real, correo electrónico, teléfono, etc., puedes empezar a usar **identidades aleatorias y únicas para cada cuenta**.

Esto hace más difícil que quienes te atacan (y las empresas tecnológicas) puedan conectar tus cuentas entre sitios y armar un perfil con todos esos pedacitos de información.

CÓMO USAR UNA IDENTIDAD ÚNICA PARA CADA CUENTA

Asegúrate de que cada uno de estos sea único para cada sitio, cuando sea posible:

- **Nombre visible:** Usa este generador de identidades aleatorias[59].
- **Nombre de usuario:** Usa este generador de identidades[59] o este generador de nombres de usuario[63] específico.
- **Foto de perfil:** Déjala en blanco o usa este generador de identidades[59]. Si usas la misma foto en todos los sitios, un atacante puede hacer una "búsqueda inversa de imágenes" para encontrar todas tus cuentas.
- **Dirección de correo electrónico** - Usa un servicio de alias de correo como:
  - Qwacky para usar alias de correo @duck.com[64] (gratis, extensión para Chrome/Firefox)
  - Proton Mail[65] (gratis/de pago)
  - Addy.io[66] (gratis/de pago)
- **Número de teléfono:** Intenta simplemente no ingresar un número de teléfono cuando te lo pidan. Si necesitas ingresar un número de teléfono solo para verificación al registrarte, intenta alquilar un número de SMSPool[67] ($0,50 por registro). Si necesitas un número de teléfono a largo plazo, considera MySudo[33].

☐ Ayuda a las personas a tu alrededor a proteger su información privada (familia, amigues, compañeres de trabajo, compañeres, vecines)

Si eres un blanco de alto riesgo, deberías evaluar la probabilidad de que otras personas en tu vida sean atacadas como parte del acoso o daño hacia ti. Esto es muy común cuando un activista aparece en la portada de las noticias. Los trolls y justicieros de derecha irán tras familiares, compañeres de casa, amigues, compañeres de trabajo, compañeres y vecines.

Escríbeles a las personas en tu vida y sugiéreles que hagan al menos la primera sección de esta guía.

Aquí está el enlace a la checklist que estás viendo ahora: https://activistchecklist.org/doxxing[30]

Tener estas conversaciones puede ser difícil a veces (sobre todo con familiares). Puede tomar tiempo explicarle a alguien por qué está en riesgo debido a las acciones que tú estás tomando.

También puede ser buena idea avisarle con tiempo a tu jefe (y a cualquier compañere de trabajo que maneje las comunicaciones, como recepción o el contacto de RR. HH.) que estás en riesgo de sufrir acoso, para que entiendan la situación si reciben llamadas o correos sospechosos o preocupantes sobre ti.

☐ Haz un plan personal de emergencia por si te amenazan en tu casa

El nivel más alto de ataque por doxxing es cuando alguien te ubica en persona en tu casa o en tu vida cotidiana para acosarte, amenazarte o intentar hacerte daño.

Sigue nuestra Lista de planificación personal de emergencia →[68]

Estas secciones de esa lista son especialmente relevantes frente a los riesgos del doxxing:

- Sección 3: Seguridad en casa
- Sección 4: Planificación de evacuación

Agrega un PIN de seguridad a tus cuentas bancarias y de teléfono celular

Tus cuentas bancarias y la cuenta de tu proveedor de telefonía celular son objetivos de alto valor donde conviene agregar protecciones extra. Algunos de estos lugares solo intentarán verificar tu identidad con tu número de teléfono, dirección y/o fecha de nacimiento. Toda esa información es del tipo que alguien podría encontrar sobre ti en internet.

Agregar un PIN u otras medidas de seguridad ayuda a asegurarte de que solo tú tengas acceso.

CÓMO AGREGAR UN PIN A CUENTAS SENSIBLES

Estas son algunas de las cuentas que vas a querer proteger.

1. Cuentas bancarias, de tarjeta de crédito, préstamos, hipoteca e inversiones
2. Tu proveedor de telefonía celular (Verizon, T-Mobile, AT&T, etc.)
3. Proveedor de internet
4. Compañías de servicios públicos
5. Seguros (salud, hogar, auto, etc.)

Cómo agregar un PIN para cada cuenta:

1. Llama a su línea de atención al cliente.
2. Pregunta si puedes agregar un PIN de verificación.
3. Genera un PIN aleatorio[52] para cada cuenta.
4. Guárdalo en tu gestor de contraseñas[23].
5. Si no puedes agregar un PIN, pregunta qué otras funciones de seguridad ofrecen para evitar que alguien se haga pasar por ti y acceda a tu cuenta.

Resumen de herramientas

En esta guía enlazamos muchas herramientas y queríamos reunirlas en un solo lugar:

- Función "Resultados sobre ti" de Google[19]: Te avisa cuando tu información personal aparece en un nuevo resultado en Google.
- EasyOptOuts[5] ($20/año): Elimina tu información de todos los sitios de "people search".
- Block Party[21]: Te guía paso a paso por los ajustes exactos que quieres cambiar en cada una de las redes sociales más populares.
- Cyd[24]: Te ayuda a eliminar o respaldar tus publicaciones de X/Twitter (y, opcionalmente, moverlas a Bluesky).
- Generador de identidad de StrongPhrase.net[59]: Te ayuda a tener un nombre/usuario/etc. aleatorio para usar en cada sitio.
- MySudo[33] o Google Voice[32]: Consigue un número de teléfono secundario para no tener que compartir tu número real.
- Qwacky para usar correo @duck.com[64], Proton Mail[65] o Addy.io[66]: Usa un servicio de alias de correo para generar una dirección única en cada sitio que no pueda cruzarse entre sitios.
- SMSPool[67]: Te permite rentar un número de teléfono aleatorio por unos minutos para recibir un mensaje de verificación cuando te registras en servicios que exigen un número.

- Optery[6] ($250/año): Para personas con alto nivel de amenaza. Hace lo mismo que EasyOptOuts, pero va un poco más lejos. (La gente suele sugerir DeleteMe, pero Optery es más efectivo.)

Nota: Las herramientas solo llegan hasta cierto punto; algunos pasos hay que hacerlos a mano.

Responder al doxxing y al acoso en línea

Todavía no tenemos una guía completa de respuesta ante el doxxing, pero sí queremos ofrecerte algunos puntos de partida.

Respuesta ante el doxxing:

1. **Prioriza tu seguridad física:** Vete a casa de unx amigx o a un lugar seguro si te preocupa estar en riesgo de daño o acoso inminente. Confía en tu instinto. Es mejor apoyarte en tu red y que no pase nada, que lo contrario.
2. **Cuida tu bienestar emocional:** Incluso el acoso supuestamente "menor" puede ser muy estresante porque no sabes si las amenazas se van a concretar. Cuídate[69].
3. **Busca apoyo:** No hagas esto solx. Ten a alguien a tu lado en cada paso.
   - Encuentra amigxs/compas que te escriban seguido y te ayuden a mantenerte con los pies en la tierra.
   - Busca apoyo experto: Línea de ayuda 24/7 de Access Now[70] (gratis), Equality Labs[71], Brightlines[53] (de alto nivel), Convocation Research & Design[54] (de alto nivel).
4. **Documenta todo:** No borres nada ni bloquees a nadie. Puede ser útil para rastrear después a quienes están detrás de los ataques. Delega esta tarea en alguien de confianza si lo necesitas. Cómo documentar[72].
5. **No llames a la policía:** Lxs policías podrían usar una investigación para aprender más sobre las redes activistas. Dicho eso, puede haber situaciones en las que leyes locales contra el acoso podrían apoyarte. Considera consultar con unx abogadx alineadx con el movimiento antes de contactar al Estado o involucrar a la policía en tu situación. Abogadxs alineadxs con el movimiento que puedes considerar: CLDC[73] (línea de respuesta rápida: 541-603-6891) o NLG[74].

Aprende más sobre cómo responder:

- Brightlines - Recursos contra el doxxing[75]
- Right To Be - Guía de respuesta ante el doxxing[76]
- Right To Be - Guía de autocuidado[69]
- PEN America - Qué hacer si has sido víctima de doxxing o te han puesto en una lista de vigilancia[77]
- PEN America - Manual de campo contra el acoso en línea - Respuesta ante el doxxing[78]
- Crimethinc - Prevención y cuidado para quienes son blanco de doxxing y acoso político[79] (2020)

Sigue aprendiendo con estas guías relacionadas

Planificación de emergencia

Arma una red de apoyo de emergencia en caso de que te detengan o te amenacen.

Seguridad en Signal

Asegura la app de mensajería Signal para tener comunicaciones más seguras.

Teléfono secundario

Configura un teléfono extra para activismo y protestas.

Protección contra spyware

Protégete del spyware y los programas de vigilancia.

Ventajas y desventajas del Modo de aislamiento 3 min de lectura 50

Póster "La poli en la puerta" 80

Enlaces

1. activistchecklist.org/es/contribute/
2. theintercept.com/2026/05/13/miami-beach-billboard-truck-david-suarez-israel-gaza/
3. aljazeera.com/amp/news/2025/7/11/canary-mission-how-us-uses-a-hate-group-to-target-palestine-advocates
4. activistchecklist.org/es/party/
5. easyoptouts.com
6. optery.com
7. fastpeoplesearch.com
8. consumerreports.org/electronics/personal-information/services-that-delete-data-from-people-search-sites-review-a2705843415/
9. innovation.consumerreports.org/wp-content/uploads/2024/08/Data-Defense_-Evaluating-People-Search-Site-Removal-Services-.pdf
10. kanary.com
11. suppression.peopleconnect.us/login
12. nationalpublicdata.com
13. nationalpublicdata.com/optout.html
14. github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List
15. clearview.ai/privacy-and-requests
16. pimeyes.com/en/opt-out-request-form
17. facecheck.id/en/RemoveMyPhotos
18. support.google.com/websearch/answer/12719076?hl=en
19. myactivity.google.com/results-about-you
20. support.google.com/websearch/answer/9673730?hl=en
21. blockpartyapp.com
22. chromewebstore.google.com/detail/block-party-%E2%80%94-deep-clean/hefhjoddehdhdgfjhpnffhopoijdfnak
23. activistchecklist.org/es/essentials/
24. cyd.social
25. digitalfootprintcheck.com/free-checker
26. kenklippenstein.com/p/ice-making-list-of-anyone-who-films
27. canarymission.org
28. nitter.net/camhigby/status/2015093531526729789
29. theguardian.com/us-news/2025/nov/21/fbi-signal-group-chat-immigration
30. activistchecklist.org/es/doxxing/
31. signal.org/blog/phone-number-privacy-usernames/
32. workspace.google.com/products/voice/
33. anonyome.com/individuals/mysudo/
34. sideline.com
35. line2.com
36. activistchecklist.org/es/signal/
37. activistchecklist.org/doxxing
38. bing.com/webmasters/tools/contentremoval
39. google.com/alerts
40. support.google.com/webmasters/answer/7041154?hl=en
41. equifax.com/personal/credit-report-services/credit-freeze
42. experian.com/help/credit-freeze/
43. transunion.com/credit-freeze
44. support.google.com/maps/answer/15439776?hl=en
45. google.com/maps
46. zillow.zendesk.com/hc/en-us/articles/202036344-How-do-I-hide-or-remove-photos-of-my-home
47. support.redfin.com/hc/en-us/articles/360002970072-Upload-Your-Home-s-Photos
48. support.apple.com/en-us/105120
49. landing.google.com/intl/en_us/advancedprotection/
50. activistchecklist.org/es/lockdown/
51. support.signal.org/hc/en-us/articles/360007059792-Signal-PIN
52. strongphrase.net/passcode
53. brightlin.es
54. convocation.design
55. accessnow.org/help/
56. instantusername.com
57. duckduckgo.com/email/
58. gmail.googleblog.com/2008/03/2-hidden-ways-to-get-more-from-your.html
59. strongphrase.net/identity
60. usps.com/manage/po-boxes.htm
61. ipostal1.com
62. ups.com/us/en/the-ups-store/mailboxes
63. strongphrase.net/username
64. github.com/Lanshuns/Qwacky
65. proton.me/support/pass-email-alias
66. addy.io
67. smspool.net
68. activistchecklist.org/es/emergency/
69. righttobe.org/guides/self-care-when-experiencing-online-harassment/
70. accessnow.org/resources/
71. equalitylabs.org/services/
72. onlineharassmentfieldmanual.pen.org/documenting-online-harassment/
73. cldc.org
74. nlg.org
75. brightlin.es/anti-doxxing-resources
76. righttobe.org/guides/responding-to-online-harassment/
77. pen.org/online-abuse-digital-safety/what-to-do-if-youve-been-doxed-or-placed-on-a-watchlist/
78. onlineharassmentfieldmanual.pen.org/respond/
79. crimethinc.com/2020/08/26/doxcare-prevention-and-aftercare-for-those-targeted-by-doxxing-and-political-harassment
80. activistchecklist.org/es/police/