INSI

Defensa Digital:

Cómo Gestionar El Acoso En Línea Dentro y Fuera de la Redacción

JOURNALISM | SAFETY | RESPONSIBILITY | COMMUNITY

Índice

Introducción

El sector de los medios de comunicación se enfrenta a una ola implacable de acoso en línea contra periodistas, perpetrado por actores estatales, redes del crimen organizado, bots y miembros del público envalentonados por el anonimato. Los discursos de odio, la desinformación y las amenazas de violencia física son una realidad diaria para muchos colegas. Algunos se ven obligados a abandonar la profesión; otros sufren secuelas psicológicas a largo plazo, justo en un momento en que el periodismo independiente y en profundidad es más necesario que nunca.

La violencia digital es notoriamente difícil de contener, pero lo que está claro es que los periodistas esperan que sus empleadores actúen antes, durante y después de los ataques, ofreciendo apoyo, sí, pero también medidas concretas.

Las organizaciones miembros de INSI se han estado reuniendo desde 2020 para compartir enfoques y lecciones aprendidas con mucho esfuerzo. La Google News Initiative y Facebook apoyaron y participaron en las primeras etapas, y reconocemos su contribución.

Esta guía —redactada para INSI por Mike Christie, uno de los principales impulsores de esta iniciativa— se basa en esas conversaciones iniciales y todas las que vinieron después. Como jefe global de seguridad de Reuters, Christie ayudó a establecer el estándar sobre cómo las Redacciones pueden proteger a su personal ante amenazas físicas, digitales y emocionales. Su labor ha sido clave para definir las buenas prácticas del sector.

Esta guía está diseñada para ayudar a los responsables de la Redacción —de los departamentos editorial, de seguridad y de recursos humanos— a crear un marco práctico que mitigue el impacto del abuso en línea y prepare a las Redacciones si las amenazas digitales se trasladan al mundo real.

Cada Redacción tiene un perfil de riesgo, una cultura y unos recursos distintos. Pero ninguna debería enfrentarse sola a la violencia digital. Una colaboración a nivel sectorial —con las plataformas, para exigir responsabilidad y aplicación de normas, y con los gobiernos, para promover una regulación significativa— tendrá mucho más impacto que los esfuerzos individuales. INSI anima a todos sus miembros a participar activamente en estas iniciativas colectivas e incorporar el espíritu de resiliencia compartida en su respuesta institucional.

Reconocemos que muchas Redacciones ya están muy familiarizadas con la magnitud y la naturaleza del acoso en línea, y que el tiempo escasea. Por eso, esta guía empieza por las medidas más urgentes y prácticas. Se abre con un marco de actuación para gestionar el acoso digital, dirigido específicamente a los responsables de la seguridad y el apoyo al personal, y después pasa al contexto general.

En los anexos, encontrará listas de verificación con estrategias clave de mitigación, como el autodoxeo y la planificación de respuestas. Esperamos que esta guía sea una herramienta útil y accesible para periodistas, responsables y profesionales de la seguridad por igual.

Contramedidas preventivas

En el mundo actual, cada vez más interconectado, los periodistas se enfrentan a riesgos crecientes a medida que los agresores aprovechan dispositivos vinculados a la nube y datos compartidos entre plataformas. Una amenaza vaga ya es preocupante, pero cuando incluye el nombre del colegio de un hijo o la foto de un dormitorio extraída de una web inmobiliaria, el peligro se vuelve mucho más real. La planificación proactiva es esencial para preparar a las Redacciones.

1. Cuantificar el problema

Realiza una encuesta en la Redacción para comprender la magnitud del acoso y abuso en línea dentro de tu organización. Asegúrate de incluir a mujeres y periodistas pertenecientes a minorías, ya que son quienes más sufren este tipo de ataques.

2. Ofrecer capacitación

Incluye contenidos básicos sobre acoso en línea, sus consecuencias y la respuesta de la empresa en todos los cursos de seguridad en entornos hostiles y capacitación en ciberseguridad. También puedes ofrecer talleres especializados centrados únicamente en el acoso digital.

3. Crear canales de notificación

Promociona los canales disponibles para denunciar casos de acoso en línea, especialmente cuando se producen por mensajería personal o redes sociales. Esto puede incluir un canal en Teams o Slack, o simplemente una dirección de correo electrónico. Considera crear un espacio donde los periodistas puedan compartir sus experiencias, lo cual puede ayudar a detectar patrones emergentes y fomentar el apoyo mutuo.
Asegúrate de que el equipo de seguridad editorial esté informado con antelación sobre cualquier cobertura que pueda desencadenar una campaña de acoso digital, en lugar de esperar a gestionar las consecuencias después.

4. Ejercicios de autodoxeo

Pide al personal que realice ejercicios básicos de autodoxeo para comprobar cuánta información sensible se puede encontrar sobre ellos en línea. Es imposible borrar todo lo que se ha acumulado durante décadas de vida digital; por ejemplo, en Estados Unidos, ser propietario de una vivienda implica que tu dirección aparece en registros públicos. No obstante, pueden estar filtrándose datos a través de perfiles sociales mal configurados. Este ejercicio debe formar parte del proceso de incorporación de nuevas personas a la Redacción.

5. Investigar a fondo

Haz un análisis más detallado de las vulnerabilidades digitales de periodistas muy visibles o que trabajen en temas delicados. El Departamento de Seguridad Informática o el personal de gestión de riesgos puede encargarse de ello o contratar a proveedores externos.

6. Usar servicios de eliminación de datos en línea

Utiliza servicios como DeleteMe para enviar solicitudes automáticas de exclusión a intermediarios de datos personales. Aunque no están disponibles en todos los países, es recomendable contratar un plan empresarial para toda la Redacción o cuentas individuales para casos concretos. Estos servicios no eliminan los datos de origen, pero sí ayudan a limitar su circulación.

7. Emplear servicios de vigilancia de amenazas

Muchas empresas de medios ya utilizan servicios de vigilancia de marca y reputación que detectan infracciones de derechos de autor, cuentas falsas o críticas que puedan dañar su imagen. También existen servicios similares para vigilar amenazas a la seguridad de la Redacción o de periodistas concretos. Algunos servicios rastrean la Internet profunda y canales cerrados como grupos de Telegram.

8. Eliminar publicaciones antiguas

Revisa y limpia publicaciones antiguas que, aunque inocentes en su momento, podrían comprometer la seguridad o integridad del periodista. Opiniones políticas del pasado — incluso si ya no se sostienen— pueden descalificar a una persona para cubrir campañas electorales. Fotos de fiestas universitarias pueden representar un problema si se cubren temas con grupos ultraconservadores. Considera incluir esta revisión en el proceso de incorporación.

9. Mantener perfiles con poca información

Una imagen sonriente puede ser útil para un reportero televisivo, pero ¿necesita un periodista económico tener su rostro en los perfiles? Las fotos pueden ser utilizadas por sistemas de reconocimiento facial. Una opción para las periodistas mujeres, quienes sufren más acoso, es crear perfiles en línea neutros en cuanto al género.

10. Separar lo personal de lo profesional

Considera separar completamente las identidades digitales personales y profesionales. Las cuentas personales deben estar restringidas a familia y amistades, con máxima privacidad, y no deben incluir a colegas ni fuentes. Las cuentas profesionales deben contener mínima información personal y centrarse en el trabajo, entendiendo que todo lo que aparece puede hacerse público o ser usado por adversarios.

11. Capacitación para apariciones públicas

Ofrece capacitación sobre cómo deben gestionar los periodistas sus intervenciones en actos públicos. Los grupos de extrema derecha, por ejemplo, suelen intentar tender trampas mediante preguntas provocadoras para luego difundir sus respuestas con el fin de desacreditarlos. También hay quienes se hacen pasar por fuentes para ofrecer primicias falsas, buscando pruebas de parcialidad que puedan dañar tu credibilidad.

12. Identificar a personas o grupos vulnerables

Algunos periodistas pueden necesitar apoyo adicional o capacitación específica, por ejemplo:

- Reporteros políticos y verificadores de datos
- Quienes trabajen en países donde el acoso digital ha sido instrumentalizado por el Estado
- Mujeres, personas de color y miembros del colectivo LGBTQ+
- Quienes tengan una alta visibilidad online; hayan sido criticados públicamente por líderes o figuras influyentes; o cubran temas geopolíticos polarizantes

13. Moderar los comentarios

Mantener un espacio de comentarios seguro y civilizado en línea es un desafío importante que requiere recursos específicos. Algunas Redacciones optan por desactivar los comentarios por completo. Otras emplean herramientas automáticas, o bien una combinación de automatización mediante IA y moderación humana.

Incluso los comentarios ofensivos dirigidos contra una empresa o su sitio web, aunque no vayan dirigidos a un periodista concreto, deben ser vigilados por si expresan la intención de cometer actos violentos en el mundo físico.

14. Crear un equipo de respuesta multidepartamental

Responder eficazmente al acoso en línea más grave puede requerir la participación de varios departamentos. Actúa con antelación y establece un protocolo para una respuesta integral. Crea un grupo de trabajo o célula de crisis que cuente con lo siguiente:

- **Dirección Editorial.** Toma decisiones sobre reubicación de periodistas, contratación de seguridad o intervención de las autoridades.
- **Seguridad Editorial.** Gestiona todas las amenazas —físicas, digitales y emocionales— que afecten al personal.
- **Seguridad Informática.** Bloquea ataques, identifica su origen, evalúa su gravedad, registra los incidentes y detecta tendencias.
- **Seguridad Corporativa.** Impide el acceso de acosadores identificados a las instalaciones.
- **Departamento Legal.** Valora acciones legales y estudia los límites relacionados con la libertad de expresión.
- **Recursos Humanos.** Ofrece apoyo emocional y psicológico; participa en decisiones sobre cambios temporales de puesto o lugar de trabajo.
- **Comunicación Corporativa.** Puede intervenir públicamente en nombre de la empresa; por ejemplo, en hilos de comentarios.
- **Apoyo entre colegas.** Se asegura de que las personas afectadas se sientan acompañadas por sus compañeros.

15. Proporcionar orientación sobre seguridad editorial

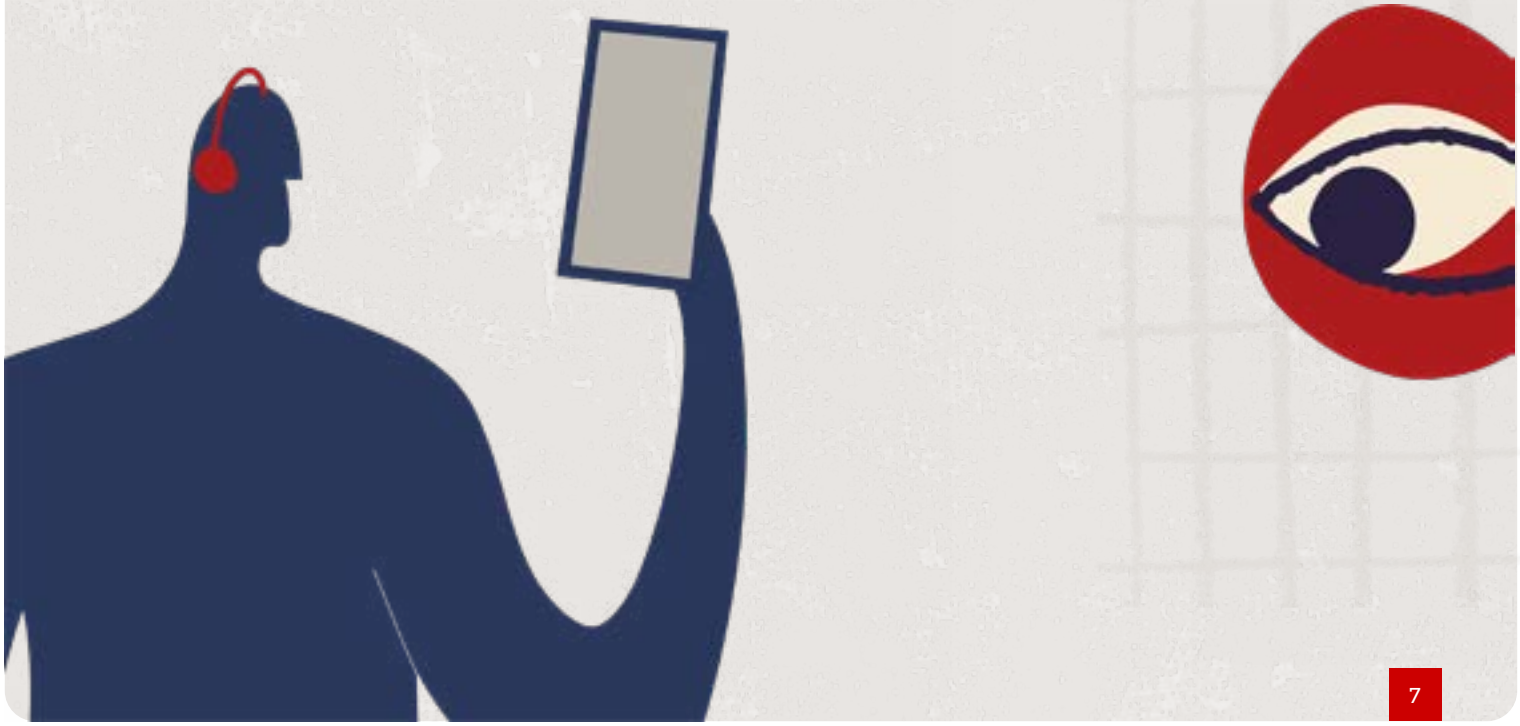
La biblioteca interna de recursos de seguridad de cualquier organización periodística debe incluir materiales sobre la naturaleza del acoso en línea, sus efectos y el apoyo que ofrece la empresa. Las recomendaciones básicas sobre ciberseguridad también deben contemplar el acoso digital.

16. Reducir el riesgo

Las políticas BYOD (Bring Your Own Device, es decir, uso de dispositivos personales) y la frecuente colaboración con periodistas freelance dificultan reducir la vulnerabilidad de las Redacciones y los periodistas. Por ejemplo, es posible que una aplicación segura utilizada para comunicarse con una fuente sensible esté tanto en la computadora portátil de la empresa como en la personal. También es posible que algunas conversaciones se guarden de forma no segura en la nube, en cuentas a las que el Departamento de Informática no tenga acceso.

Hay formas de reducir el riesgo, entre ellas las siguientes:

- Publicar las historias más delicadas sin firma. Aunque esta opción suele generar resistencia entre periodistas (y sus preferencias deben respetarse), puede ser una medida eficaz de protección.
- Revisar las políticas que permiten mostrar perfiles detallados de periodistas en la web corporativa, o enlazar sus perfiles sociales en artículos. Aunque estas prácticas pueden favorecer la marca personal, también aumentan la cantidad de información sensible disponible públicamente, como las fotos, que pueden ser utilizadas por sistemas de reconocimiento facial.
- Revisar los ajustes, porque los mismos ajustes que permiten que una noticia se viralice pueden ser usados para acosar. Las Redacciones deben establecer recomendaciones sobre cómo configurar adecuadamente estos ajustes, usándolos de forma segura y estratégica.



Mecanismos de denuncia

Fomentar la confianza entre periodistas

El acoso en línea no siempre llega a través de canales controlados por la empresa, como publicaciones visibles o correos corporativos. A menudo, se produce mediante mensajes privados enviados a las cuentas personales de redes sociales de los periodistas.

Aunque los periodistas deberían denunciarlo, muchas veces no lo hacen. Entre las razones más comunes es que lo ven como "parte del trabajo"; temen que se cuestione su integridad, profesionalidad o credibilidad; o tienen miedo de ser retirados de una historia relevante. Por eso es fundamental fomentar una cultura activa de denuncia del abuso. Algunas acciones clave son las siguientes:

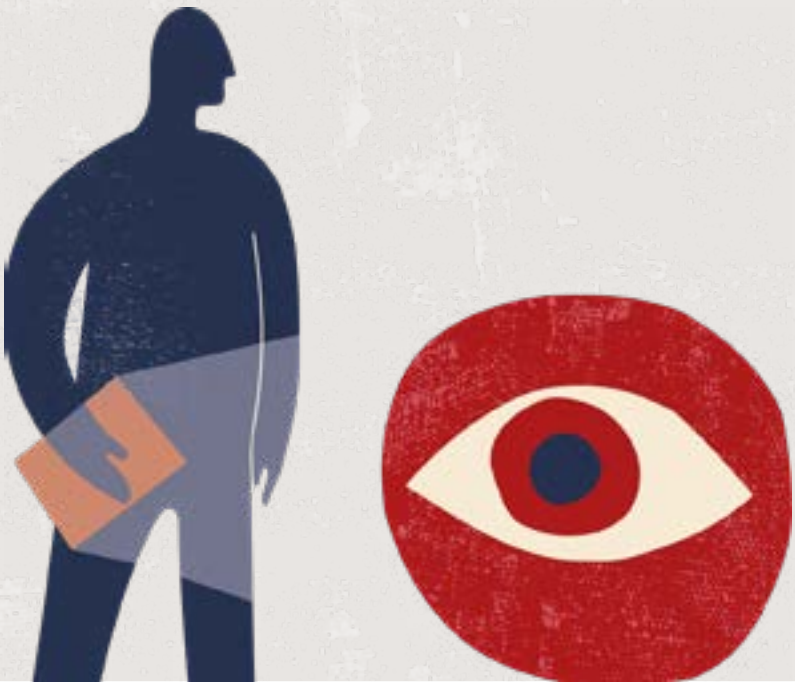
- **Capacitación y sensibilización.** Los periodistas no deben minimizar la gravedad del acoso digital. La capacitación debe incluir cómo piensa actuar la empresa ante este tipo de ataques, enfatizar cómo se apoyará a las personas afectadas y garantizar que no se les excluirá de una cobertura por haber denunciado el acoso.
- **Establecer canales de notificación eficaces.** Puedes utilizar Teams, Slack Forms o el correo electrónico. Da seguimiento a los mecanismos de denuncia, pues de lo contrario los periodistas perderán la confianza en el proceso.

Denunciar abusos ante las plataformas

Algunas redes sociales han habilitado portales especiales para socios de confianza, que permiten denunciar incidentes como cuentas hackeadas, robo de credenciales, acoso en línea y otros problemas relacionados. En algunos casos, existe incluso un contacto directo dentro de la empresa de redes sociales al que las organizaciones pueden dirigirse en caso de emergencia.

En otros casos, son los propios usuarios quienes deben reportar los incidentes de acoso u otros problemas directamente a la plataforma de redes sociales.

Los gestores deben tener claro qué plataformas utilizan sus periodistas y cómo responde cada plataforma a las quejas.handle complaints.



Mecanismos de vigilancia

El acoso en línea públicamente visible puede vigilarse mediante herramientas que permiten a las organizaciones de noticias detectar amenazas más amplias a sus Redacciones e instalaciones. Muchas de estas herramientas están orientadas a la protección de la marca. Algunas pueden explorar la web oscura y profunda, y quizás los chats de grupo de aplicaciones como Telegram, además de la internet pública.

Algunos productos más recientes pueden utilizarse para vigilar amenazas o ataques que se canalizan a través de mensajes directos, pero requieren el consentimiento del periodista para incluir sus cuentas personales de redes sociales en este tipo de vigilancia.

Otra opción son las herramientas de filtrado automatizado que buscan proteger a los periodistas (y a otros usuarios de internet) del impacto tóxico de los mensajes de odio. Estas herramientas pueden utilizarse para ocultar mensajes con ciertas palabras o contenido.

Este tipo de moderación de contenido puede ser beneficioso, ya que protege a los destinatarios de parte del daño emocional, pero también podría impedir que una organización detecte amenazas graves que requieran una respuesta. Existen nuevas versiones basadas en IA que protegen al destinatario de mensajes desagradables y revisan los mensajes para identificar amenazas que deben denunciarse.

Mecanismos de respuesta

Una vez que se han establecido mecanismos eficaces de denuncia y vigilancia, las Redacciones pueden enfrentarse al reto de analizar cientos de mensajes para determinar cuáles podrían tener consecuencias reales en el mundo físico. Clasificar el acoso en línea para identificar a los verdaderos agresores con historial violento o delictivo puede ser como buscar una aguja en un pajar.

Tener en cuenta lo siguiente al decidir cómo responder:

1. Identificar a los atacantes

Google puede ser un buen punto de partida y ofrecer resultados reveladores. Muchos agresores utilizan los mismos alias en distintas plataformas, lo cual facilita su rastreo. Herramientas como Social Catfish permiten hacer búsquedas inversas por correo electrónico. PeekYou puede rastrear alias y nombres de usuario en foros y redes.

El Departamento de Seguridad Informática de una empresa de medios también puede tener la capacidad de determinar la ubicación de las direcciones IP. Muchos atacantes en línea utilizan VPN para ocultar su ubicación y abren cuentas falsas cuando una es desactivada.

2. Análisis y clasificación de amenazas

Algunos indicios de que una amenaza en línea puede derivar en violencia física son:

- **Implica una amenaza directa como "te mataré".** Por el contrario, una amenaza indirecta como "deberías ser ejecutado por traición" puede interpretarse como libre expresión y no como una intención de hacer daño.
- **Aumenta el riesgo para un periodista.** ¿Se ha revelado su domicilio? ¿Estaría en peligro si se hiciera pública su ubicación?
- **El atacante oculta su identidad.** Esto podría indicar que sabe que sus acciones son incorrectas. Los atacantes que usan sus nombres reales pueden, contrariamente a lo que se cree, representar una mayor amenaza, ya que podrían no comprender que lo que hacen es incorrecto.
- **Ubicación.** Alguien que viva cerca puede ser una amenaza mayor que alguien que necesita volar al otro lado del mundo para llegar a su objetivo.
- **Antecedentes penales o de violencia.** ¿Tiene el agresor vínculos con grupos violentos o permiso para portar armas?
- **Escalada.** ¿Los ataques se han propagado de una plataforma a otra y han aumentado en volumen y estridencia?

- **Organizado.** ¿Está el gobierno u otra entidad involucrada en los ataques? ¿Han demostrado previamente su disposición a usar la violencia? ¿Podría el gobierno también emprender acciones legales o detener a un periodista?
- **Bots.** Esté atento a cuentas nuevas sin historial claro o que hayan participado en campañas similares.

3. Proteger a las personas afectadas

Bloquear a un agresor en línea puede parecer una medida lógica para proteger la salud mental del periodista. Sin embargo, el bloqueo directo puede provocar una escalada: el atacante puede crear nuevas cuentas para continuar con el acoso desde el anonimato, fuera del radar de la víctima.

Como alternativa, el equipo de seguridad editorial o el Departamento de Informática podrían asumir la vigilancia de las cuentas personales de redes sociales. No obstante, algunos periodistas pueden mostrarse reacios a facilitar sus contraseñas o a otorgar el acceso a mensajes de fuentes confidenciales.

En estos casos, un colega o superior editorial podría vigilar temporalmente los mensajes, involucrando al equipo de seguridad o informática si es necesario.

4. Actuar con rapidez

Las Redacciones deben reaccionar sin demora cuando se determine que una situación de acoso digital puede derivar en un riesgo real. Entre las medidas recomendadas:

- **Llamar a las autoridades.** Las amenazas directas siempre deben notificarse a la policía o a los organismos gubernamentales. Los periodistas podrían tener que presentar la denuncia ellos mismos.
- **Cerrar** las oficinas.
- **Agregar atacantes conocidos a las listas de personas a las que se les niega el ingreso** a las oficinas de la empresa e informar a los proveedores externos y propietarios.
- **Garantizar la seguridad del domicilio o alojamiento temporal del periodista** proporcionándole un sistema de seguridad para el hogar o suscribiéndolo a un servicio de seguridad.
- **Trasladar al periodista y a su familia a un hotel con buena seguridad** mientras se evalúa la amenaza.
- **Contratar guardaespaldas** para talentos de alto perfil.
- **Redirigir el correo electrónico corporativo y bloquear las cuentas infractoras** en el correo electrónico personal.
- **Decidir quién debe vigilar las amenazas entrantes** en nombre del periodista.
- **Denunciar al infractor ante la plataforma.** Los periodistas podrían tener que presentar una denuncia a través de las herramientas de autodenuncia de la plataforma.
- **Emprender acciones legales.**
- **Ponerse en contacto con periodistas** de otras organizaciones que puedan tener información para ayudar a evaluar la gravedad de la amenaza.
- **Apoyar públicamente al periodista** para reforzar su resiliencia y moral.
- **Denunciar el acoso.** Esta podría ser una forma saludable de llamar la atención sobre un ataque, especialmente si forma parte de una tendencia más amplia.

5. Apoyar al periodista

Ser blanco de una campaña de acoso puede tener un impacto emocional profundo. El apoyo institucional es esencial para mantener la resiliencia y ayudar al periodista a seguir informando sin miedo. Algunos mecanismos de apoyo son:

- **Ofrecer apoyo y asesoramiento por parte de los compañeros dentro de la organización.**
- **Aclarar que la empresa no culpa al periodista** ni a su labor periodística y que lo apoyará para que continúe cubriendo la noticia.
- **Brindar asistencia para denunciar el acoso** en redes sociales o presentar una denuncia policial.
- **Analizar a fondo las vulnerabilidades en línea del periodista afectado** para asegurarse de que los atacantes no puedan seguir explotándolo.
- **Revisar y mejorar la seguridad del domicilio del periodista.** Decidir si se debe trasladar al periodista y a su familia a un lugar más seguro.
- **Redirigir la atención del acosador hacia la empresa.** Añadir declaraciones oficiales a una cadena de comentarios o publicar un comunicado.

6. Casos extremos

Algunos casos de acoso en línea pueden escalar hasta el punto de poner en riesgo la seguridad física de toda la Redacción. Una campaña organizada y deliberada por parte de una figura política popular para fomentar la ira y el odio podría hacer inseguro el trabajo periodístico en público, en ciertos eventos o en ciertas regiones. Los equipos de seguridad deben estar atentos a esta posibilidad y dispuestos a elevar los casos individuales de acoso a la alta dirección.

7. Documentar los casos y aprender de ellos

Cada nuevo caso de acoso en línea puede ser diferente y puede dejarle lecciones sobre cómo responder a futuros ataques. Llevar registros le permitirá a su organización identificar tendencias emergentes. Esto será fundamental para persuadir a la alta dirección y a los directores financieros a asignar fondos para combatir el problema.

Lista de verificación para responsables de la Redacción

Contramedidas preventivas	Cuantificar el problema	Realizar una encuesta al personal
	Ofrecer capacitación y sensibilización	Incluir en cursos básicos de seguridad para todos los periodistas
	Establecer canales de comunicación	Teams, Slack, correo electrónico
	Realizarse pruebas de autodoxeo	Incluir en el proceso de incorporación y poner a disposición de la Redacción a través de un módulo de autoaprendizaje publicado en la red interna
	Investigar a fondo	Considerar utilizar un proveedor externo
	Contratar servicios de eliminación de datos	Suscribirse a un servicio de eliminación de datos para periodistas en riesgo
	Vigilar las amenazas	Los proveedores externos pueden explorar la web oscura y profunda y áreas menos accesibles, como los grupos de chat de Telegram
	Borrar las publicaciones antiguas	Incluir en el proceso de incorporación
	Crear perfiles con pocos detalles	Incluir en el proceso de incorporación y en la capacitación en seguridad
	Crear cuentas personales y profesionales	Analizar la separación de perfiles personales y profesionales con periodistas y equipos editoriales
	Dar seguimiento a grupos o individuos vulnerables	Realizar un taller de seguridad adicional para el equipo de verificación de datos y los equipos políticos, posiblemente presentado por un proveedor externo
	Ofrecer capacitación sobre apariciones en público	Proporcionar capacitación sobre cómo los periodistas deben manejar las apariciones en público
	Participar en la moderación de comentarios	Un proveedor externo podría proporcionarlo
	Establecer un equipo de respuesta multidepartamental	Incluir gestión editorial, seguridad, editor de redes sociales, legal, apoyo entre pares
	Ofrecer orientación sobre seguridad editorial	Publicar en la red interna
	Reducir los riesgos	Eliminar fotos de los perfiles de periodistas

Lista de verificación para responsables de la Redacción

Mecanismos de denuncia	Establecer un canal para que los periodistas denuncien el acoso	Utilizar Teams, Slack, correo electrónico
	Utilice canales para denunciar abusos en las plataformas	Algunas de las opciones son portales para socios, contactos directos en plataformas y denuncias individuales de periodistas
Mecanismos de vigilancia	Vigilar las amenazas públicas	Valorar la posibilidad de contratar un proveedor externo
	Vigilar los mensajes directos	Valorar la posibilidad de contratar al mismo proveedor externo, si el periodista está de acuerdo
	Utilizar software que proteja a los periodistas de los mensajes de odio	Esto protege a los objetivos de parte del daño emocional, pero también podría impedir la detección de amenazas graves
	Moderar y vigilar los hilos de comentarios	Valorar la posibilidad de contratar un proveedor externo
Mecanismos de respuesta	Elaborar un método para identificar atacantes en línea	Social Catfish permite realizar búsquedas inversas de direcciones de correo electrónico. PeekYou permite realizar búsquedas por nombre de usuario
	Evaluar y priorizar las amenazas	Equipo de seguridad, posiblemente apoyado por un proveedor externo
	Proteger a los objetivos	Pedir a los editores y colegas vigilar los mensajes si es necesario
	Actuar ante amenazas graves	Revisar la seguridad del periodista acosado; informar a la administración del edificio; comunicarse con las autoridades; ayudar a los periodistas a denunciar amenazas; comunicarse con las plataformas; decidir sobre las opciones legales; los colegas se ponen en contacto con el periodista objetivo y con cualquier colega afectado por el ataque
	Ofrecer apoyo	El gerente directo o los compañeros pueden ser los más indicados para apoyar al periodista afectado
	Llevar un registro	El Departamento de Seguridad Informática puede tomar la iniciativa

Anexo 1. Definir el acoso en línea

El acoso y el abuso en línea pueden adoptar diversas formas y su objetivo es acosar, intimidar o silenciar a los periodistas. Puede extenderse al ámbito físico y causar daño emocional a sus víctimas, con consecuencias de gran alcance.

Conforme la tecnología evolucione y la inteligencia artificial se vuelva más sofisticada, nos enfrentaremos a nuevas formas de acoso en línea a través de canales de difusión que hoy apenas conocemos. Es poco probable que las plataformas en las que actualmente ocurre el acoso y el abuso más tóxicos sean las que más nos preocupen en los próximos años.

Adoptar una postura más defensiva y emplear estrategias proactivas que fomenten la resiliencia es más útil que centrarse en plataformas específicas o depender de ellas para gestionar las denuncias de abuso. El acoso en línea también puede caer en el debate sobre la libertad de expresión, lo que dificulta la intervención de las autoridades y hace que las empresas de redes sociales se muestren reacias a asumir la responsabilidad de la moderación del contenido.

Puedes encontrar otras definiciones de acoso en línea aquí: PEN America; Harvard T.H. Chan School of Public Health; Dart Center for Journalism & Trauma

Por qué es importante

Las Salas de Redacción deben proteger a sus periodistas del acoso en línea para:

- Garantizar que puedan informar las noticias con libertad, sin miedo y de manera objetiva.
- Protegerlos a ellos y a su lugar de trabajo de amenazas físicas.
- Apoyar su salud mental y bienestar emocional a largo plazo.

Uno de los principales objetivos del acoso en línea es silenciar a los periodistas, disuadirlos de informar sobre temas relevantes o hacerlos abandonar la profesión por completo. Suele ser efectivo. Una encuesta realizada en 2020 por la UNESCO entre mujeres periodistas reveló que el 30 por ciento se había autocensurado en redes sociales luego de recibir ataques en la Internet. Otra encuesta, de la International Women's Media Foundation (IWMF), reveló que el 40 por ciento de las mujeres periodistas había dejado de escribir sobre temas que ellas sabían que generarían ataques, y un tercio de ellas había pensado en dejar la profesión.

Esto convierte el acoso en línea en una amenaza corrosiva para la libertad de expresión, así como en una amenaza existencial para los periodistas y las Redacciones que exigen cuentas a los poderosos mediante un periodismo de calidad y valientes investigaciones. En todos los casos, el acoso en línea tiene el potencial de dañar psicológica y emocionalmente a sus víctimas, dejando secuelas mentales duraderas.

En algunos casos, los ataques en línea pueden derivar en violencia física y amenazas directas. La encuesta de la UNESCO reveló que el 20 por ciento de los encuestados a nivel mundial reportó haber sido atacados físicamente en el mundo real en relación con la violencia en línea sufrida. En Oriente Medio, esa proporción fue aún mayor: más de la mitad de las periodistas de la región que declararon haber sido abusadas en línea en la encuesta de la UNESCO también habían sido atacadas físicamente.

El empleo del acoso en línea como arma

El acoso en línea se ha convertido en un arma en muchos países como herramienta de censura y opresión. Gobiernos autocráticos, grupos extremistas, operadores políticos o individuos poderosos e inescrupulosos lo han utilizado para movilizar a multitudes en línea contra supuestos oponentes o críticos. El impacto de mil mensajes amenazantes o insultantes es mucho mayor que el de unos pocos.

Mujeres periodistas y periodistas procedentes de minorías

Las mujeres, periodistas de minorías y periodistas no binarios sufren mucho más abuso en línea que sus compañeros blancos, y ese acoso en gran parte tiene carácter misógino o racista. Cuando un medio de comunicación desee determinar el grado de abuso en línea que sufren los miembros de su Redacción, debe asegurarse de sondear a sus periodistas mujeres, de minorías y de la comunidad LGBTQ+, ya que es probable que sean las principales víctimas.

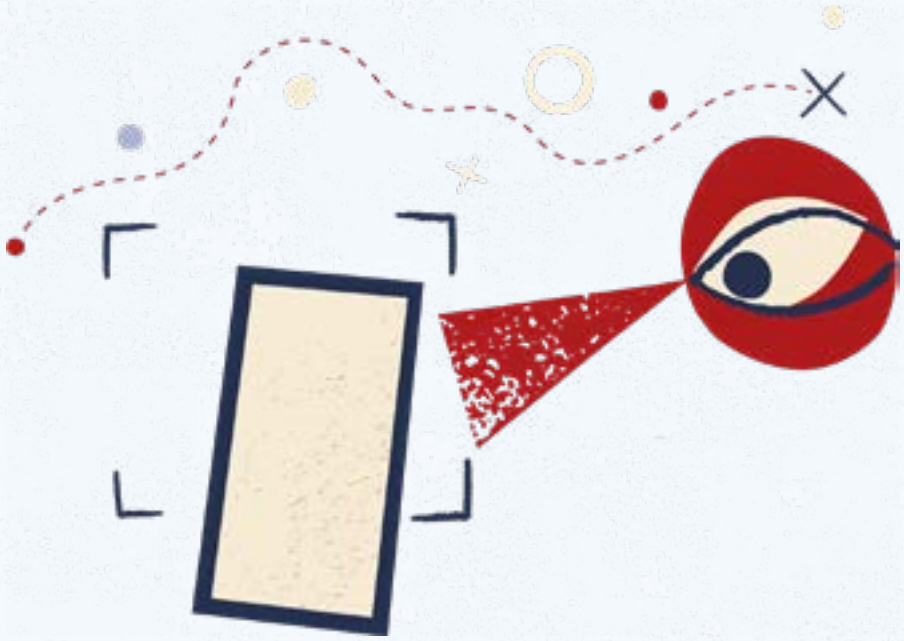
Temas que atraeb el odio en linea

Las noticias políticas en países polarizados como Estados Unidos son un foco de ataques en línea. Los países gobernados por autócratas o regímenes ilegítimos a menudo reprimen la disidencia y buscan utilizar el acoso en línea como arma para silenciar a la población.

En zonas donde las rivalidades étnicas, tribales o sectarias han provocado conflictos, la información considerada crítica hacia una de las partes o que utiliza un lenguaje percibido como parcial puede generar reacciones. Este es un problema común cuando las historias son traducidas por editores ajenos al contexto local, quienes pueden no ser sensibles a los matices del lenguaje.

Los juegos en línea, las inversiones amateur y basadas en memes, los deportes y la música pop son temas que despiertan pasiones y generan una cantidad sorprendente de abuso en línea. Otros temas del mundo real que a menudo conducen a espacios en línea tóxicos son:

- La extrema derecha y la extrema izquierda
- La misoginia
- El antisemitismo
- Las guerras culturales
- La desinformación
- El racismo
- Los debates sobre la libertad de expresión frente a la censura
- Las tensiones geopolíticas



TIPOS DE ATAQUES EN LÍNEA

Amenazas de daño

Amenazas de ejecución, sometimiento a la justicia, violación, asesinato, persecución o ataque a familiares, incluidos niños. Algunas son amenazas directas que podrían justificar una respuesta policial, pero la mayoría de las amenazas no alcanzan a convertirse en delito o se amparan en la libertad de expresión.

Ataques cibernéticos de turbas

Incitar a otros a atacar a alguien en una campaña coordinada. Esto puede implicar que numerosos acosadores denuncien la cuenta de un periodista por infringir las condiciones de servicio de una plataforma para que la eliminen. Gobiernos, ejércitos o partidos políticos pueden utilizar grupos de troles semioficiales para generar un ataque de turbas.

Ciberacoso

Hostigamiento e intimidación a una víctima durante un período prolongado. Los acechadores pueden recurrir a la vigilancia, el robo de identidad y otros actos de ciberacoso. El ciberacoso suele ser un delito penal y los periodistas víctimas deben obtener asesoramiento legal, ya que los acechadores pueden ser inestables mental o emocionalmente.

Doxeo

Divulgación de información personal sensible, como la dirección particular o el nombre del colegio de un niño. Los agresores pueden publicar esta información personal para incitar a otros a acosar, vigilar, agredir físicamente o suplantar la identidad de un periodista. El doxeo puede ocurrir mientras un periodista realiza una misión de alto riesgo en un lugar potencialmente peligroso.

Suplantación de identidad en línea

Creación de cuentas falsas en redes sociales para publicar mensajes despectivos o provocadores con el objetivo de dañar la reputación de la víctima o fomentar un acoso más amplio. Otros objetivos podrían incluir el fraude financiero o influir en la opinión pública.

Swatting

Elaborar una denuncia falsa sobre un delito, como un asesinato o una toma de rehenes, para que la policía allane la casa de un objetivo. En Estados Unidos, los equipos SWAT de la policía están fuertemente armados y se espera que sean atacados, por lo que los allanamientos pueden ser extremadamente peligrosos y, a menudo, provocan muertes.

Anexo 2. Guía para periodistas ante la violencia digital

Las amenazas y el acoso en línea están diseñados para silenciar a los periodistas y obligarlos a autocensurarse. Recibir una avalancha de amenazas puede ser aterrador y tener un impacto emocional. Los ataques en línea también pueden derivar en violencia física.

Informa a tu supervisor o editor si sufres un ataque grave.

Aumenta tu resiliencia al acoso en línea minimizando la cantidad de información personal disponible sobre ti en línea. Una amenaza general ya es bastante grave, pero es incluso peor si un atacante sabe a qué escuela va tu hijo o cuál es tu domicilio.

Hazte una prueba de autodoxeo y bloquea la configuración de privacidad de tus cuentas de redes sociales.

Considera crear perfiles públicos y privados separados en línea, minimizando la cantidad de información personal que compartes con el mundo a través de tus cuentas profesionales y reservando las personales solo para familiares y amigos.

Seguridad de la información

Actualizar tu software y aplicaciones

Constantemente se descubren vulnerabilidades en el software que alimenta nuestras computadoras y teléfonos, y los hackers y delincuentes se apresuran a explotarlas. Esto aplica por igual a nuestros teléfonos, computadoras portátiles y computadoras de escritorio. Cuida también tus computadoras y teléfonos personales y asegúrate de que todo tu software esté actualizado.

Nunca hacer clic en enlaces sospechosos

Más del 75 por ciento de los ciberataques se producen a través de correos electrónicos de phishing que contienen un enlace o archivo adjunto que vulnera tu computadora. Si un correo electrónico te informa de que algo es realmente urgente, te pide que introduzcas los datos de tu cuenta o tiene una ortografía extraña, contacta a tu Departamento de Informática o utiliza un programa como Dangerzone para abrir el archivo adjunto de forma segura o en un entorno de pruebas.

Usar un gestor de contraseñas

Los programas comerciales para descifrar contraseñas pueden adivinar cientos de millones de contraseñas por segundo y contener información sobre una persona específica de sus cuentas de redes sociales. Considera usar un gestor de contraseñas como 1Password, Dashlane o KeePassXC para generar contraseñas aleatorias para cada cuenta y guardarlas de forma segura. Asegúrate de que tu contraseña maestra sea difícil de descifrar.

Comprobar si te han hackeado

El sitio web have i been pwned? muestra cuáles de tus cuentas han sido vulneradas. Cambia la contraseña de las que hayan sido hackeadas.

Utilizar la autenticación de dos factores

Activa la autenticación de dos factores. Esto te envía un código de acceso adicional por SMS o mediante una aplicación como Google Authenticator o VIP Access de Symantec. Es preferible usar una aplicación, ya que los mensajes SMS pueden ser interceptados si clonan tu tarjeta SIM.

Evaluar periódicamente las amenazas a la seguridad de la información

Tal vez no creas que tu noticia es sensible, pero no siempre se puede predecir si la noticia puede derivar en algo sensible que deba protegerse. Considera la seguridad de la información desde el inicio de una cobertura y adopta las medidas básicas de seguridad descritas en este documento mucho antes de que una noticia de rutina se vuelva altamente sensible y requiera medidas de seguridad adicionales.

Conseguir un teléfono desechable

Considera si debes llevar tu teléfono habitual a las reuniones con tus fuentes si estás informando sobre una noticia delicada. Rastreadores expertos podrían usar tu teléfono para ubicarte a ti y a la fuente en el mismo lugar, lo cual pondría en riesgo la seguridad de ambos. Habla con tu supervisor, editor o Departamento de Informática sobre si debes usar un teléfono desechable, o "burner phone".

Conectarse con una VPN

Usa una VPN (que encripta tu conexión a internet) cuando conectes tus computadoras portátiles del trabajo y personales, y tu teléfono, a puntos de acceso wifi públicos poco seguros en hoteles y aeropuertos. Proton VPN es una buena opción gratuita.

Usar una aplicación encriptada para comunicaciones sensibles

WhatsApp, Signal o Wire son buenas opciones, aunque Meta, la aplicación propietaria de WhatsApp, conserva los llamados "metadatos" (con quién te comunicaste y cuándo), aunque no la esencia de tus chats. Telegram no se encripta automáticamente a menos que selecciones la opción de chat secreto.

Encriptar tu disco duro

El disco duro de tu computadora portátil debería estar encriptado por defecto. De lo contrario, se puede acceder fácilmente a la información de tu computadora. Si está encriptado y la computadora está apagada, la información está segura. Lo mismo ocurre con los teléfonos.

Utilizar versiones seguras de los sitios web

Siempre asegúrate de que los sitios web que visitas sean seguros. Utiliza el complemento o "plug-in" HTTPS Everywhere para asegurarte de utilizar la versión segura de los sitios web. Evita los sitios web que solo tengan "http://" en lugar de "https://" al principio de su dirección.

Encriptar archivos y documentos confidenciales

VeraCrypt y 7-Zip son programas de encriptado gratuitos y de código abierto para encriptar carpetas y archivos.

Evitar las estaciones de carga USB

Carga siempre tu teléfono en un enchufe y no en una estación de carga USB pública. En Brasil, durante el Mundial de 2014, algunos puntos de carga USB en el aeropuerto de Río fueron instalados por una banda criminal que sustraía información de los teléfonos de los viajeros. Consigue un bloqueador de datos para asegurarte de que tu teléfono solamente reciba corriente al conectar un cable USB desde una estación de carga pública.

Proteger tus dispositivos

Mantén tus teléfonos y computadoras portátiles a la mano cuando trabajes con informes confidenciales. Si dejas una computadora portátil en la habitación de un hotel, no hay forma de saber si alguien accedió a la computadora cuando tú no estabas.

Usa aplicaciones que detecten si tu teléfono ha sido atacado por malware, como iVerify, que permite a los usuarios realizar un análisis profundo gratuito una vez al mes, y la aplicación Mobile Security de F-Secure (anteriormente Lookout Lite). El malware instalado en la memoria a corto plazo suele eliminarse reiniciando el dispositivo.

Tener especial cuidado al cruzar fronteras

Guarda la información confidencial en la nube antes de cruzar la frontera. Cierra la sesión en tus cuentas o aplicaciones por si un agente fronterizo solicita acceso a tu teléfono o portátil. Apaga tus dispositivos para dificultar el acceso a la información.

Enfrentar el doxeo

La información publicada en línea puede hacernos vulnerables ante quienes rechazan nuestras historias. Los agresores podrían buscar publicaciones antiguas en redes sociales que socaven nuestra credibilidad como periodistas o revelen datos personales como la dirección particular, con la esperanza de que la información que publiquen incite a otros a atacarnos físicamente. Los troles pueden intentar obtener información sensible o comprometedora para intimidar o castigar a los periodistas.

- Pueden hacerte swatting, llamando a la policía y denunciando una situación de rehenes falsa
- Una crítica cultural feminista que desafió la dominación masculina de la industria del juego enfrentó amenazas de violación, bombas y muerte
- Un trol también puede convertirse en un acosador en la vida real.

Quizás necesites "doxearte" (lo que se conoce como "autodoxeo") para comprobar qué información tuya está en la Internet y pudiera ser usada por los troles. Valora seguir estos pasos:

Hacer una búsqueda en Google

Haz búsquedas en distintos buscadores como Google, Bing, Yandex, DuckDuckGo y Baidu. Cada búsqueda puede dar diferentes resultados, en particular si has vivido en el extranjero.

"nombres apellidos" o "nombre de usuario"	Usa comillas para buscar una palabra exacta o un conjunto de palabras. Busca diferentes combinaciones de tu nombre, nombres de usuario frecuentes y direcciones de correo electrónico.
1. "nombres apellidos" - "nombre de tu medio" 2. "nombres apellidos" "nombre de tu medio" - sitio:nombredetumedio.com	1. Esto excluirá los resultados que incluyan tu medio de noticias "nombredetumedio", mostrando resultados ocultos en páginas posteriores. El signo "menos" también es una buena manera de eliminar resultados sobre otras personas con tu mismo nombre. 2. Busca páginas que te mencionen a ti y a tu empresa de medios, y filtra las páginas de tu sitio web "nombredetumedio.com".
"primer nombre * primer apellido"	El asterisco equivale a cualquier término comodín; por ejemplo, tu segundo nombre o la inicial de tu segundo nombre
"(650) 656-5656" OR "6506565656"	Busca tu número de teléfono. Utiliza formatos alternativos.
"nombredeusuario@gmail.com" filetype:pdf	Esto mostrará cualquier archivo PDF que incluya tu correo electrónico personal; por ejemplo, publicaciones para exalumnos o presentaciones anteriores.
"primer nombre * primer apellido" 101 Main St Los Ángeles CA	Busca vinculaciones con direcciones antiguas, ciudades, pueblos, instituciones, trabajos, publicaciones
nombres apellidos site:reddit.com	Busca en sitios específicos para encontrar resultados no indexados por los buscadores.

Realizar una búsqueda inversa de imágenes

- Usa la búsqueda de imágenes de Yandex para buscar fotos tuyas. Sube una imagen tuya usando la búsqueda inversa de imágenes de Yandex.
- Sube tus fotos de perfil de X, Facebook, LinkedIn e Instagram a TinEye para ver dónde más se usan.

Bloquear la configuración de privacidad de las redes sociales

Las plataformas de redes sociales recopilan información sobre ti para vender publicidad. Controla cómo usan esta información y cuánta recopilan ajustando tu configuración de privacidad. Recuerda que la configuración de privacidad cambia y puede que necesite actualizarse.

Facebook

Comienza con la herramienta de autoayuda de privacidad de Facebook:

- Escribe "Revisión de privacidad" en el campo de búsqueda de la página de inicio y haz clic en "Visitar".
- Revisa quién puede ver los detalles de tu perfil. Asegúrate de que ninguno sea "Público".
- Limita quién puede ver tus publicaciones a "Amigos", "Amigos específicos" o "Solo yo".
- Recuerda que tu foto de portada siempre es pública. Reemplázala por una que no muestre tu rostro.

Realiza estos pasos adicionales en el "Registro de actividades":

- Haz clic en "Usar registro de actividad" para revisar tu cronología. Oculta o elimina cualquier cosa que quieras ocultar. Asegúrate de que no haya fotos en "Revisión de fotos". Las fotos aparecerán aquí si has activado el reconocimiento facial, que puedes desactivar.
- Haz clic en "Actividad en la que te han etiquetado" para ver quién te ha etiquetado. Dependiendo de la configuración de privacidad de la persona que publicó la publicación, esta podría ser pública.

Luego

- Vuelve a la página de "Privacidad" y haz clic en "Limitar últimas publicaciones".
- Revisa quién puede ver las aplicaciones que usas y cómo pueden descubrirte.
- Revisa la configuración de privacidad de tus amigos. Tus comentarios o "Me gusta" en sus páginas, y sus comentarios y "Me gusta" en las tuyas, podrían ser visibles. Incluso si no te etiquetan, quienes realmente se dedican a esto pueden ver a través de personas relacionadas contigo, como familiares y compañeros de trabajo, o personas que hayan interactuado con las partes públicas de tu página de Facebook, como darle "Me gusta" a tu foto de portada o de perfil.
- Asegúrate de que te sientes cómodo con la configuración de "Anuncios".
- En "Perfil y etiquetado", activa la opción para revisar las publicaciones en las que te etiquetan antes de que aparezcan en tu cronología.
- Comprueba cómo se ve tu perfil ante los demás mediante la función "Ver como".

Instagram

Crea una cuenta profesional de Instagram y bloquea por completo tu cuenta personal/privada, limitándola a amigos y familiares.

- Cambia tu cuenta a "Cuenta privada" para que solo quienes tú apruebes puedan ver tus publicaciones.
- Desmarca "Mostrar estado de actividad" en mensajes y respuestas a historias para que nadie pueda ver cuándo estás conectado.
- En la página "Editar perfil", desmarca la opción para permitir que tu cuenta se sugiera en otros perfiles.
- Los permisos de ubicación se controlan en la configuración de privacidad y seguridad de la aplicación de tu teléfono. Desactiva el acceso a la ubicación o limítalo a cuando quieras compartir.
- Revisa las opciones de tus mensajes e historias en los controles "Etiquetas y menciones" y "Comentarios".

LinkedIn

Dado que LinkedIn es una herramienta profesional para establecer contactos, se trata de un perfil público con foto, visible para todo el mundo. Sin embargo, las agencias de inteligencia suelen crear cuentas falsas y luego se conectan contigo y revisan tus redes de contactos. LinkedIn también se ha convertido en una plataforma popular para estafadores que, por ejemplo, anuncian ofertas de empleo falsas.

Algunas opciones para proteger tu perfil son:

- En "Visibilidad de tu perfil y red" en "Configuración y privacidad", asegúrate de que te sientas cómodo con la cantidad de personas con las que compartes tu nombre, contactos y región.
- Revisa quién puede ver tus contactos. Si te has conectado con fuentes sensibles, limítalo a "Solo tú".
- Selecciona "Modo privado" para que no lo vean las personas cuyos perfiles visitas.
- Limita quién puede ver tu correo electrónico a "Conexiones de primer grado".

Luego

- Selecciona "No" en "Visibilidad del perfil fuera de LinkedIn" si no quieres que tu perfil aparezca en otras plataformas asociadas.
- Gestiona quién puede ver tu perfil a través de tu correo electrónico o número de teléfono si no está conectado contigo.
- En "Visibilidad de tu actividad en LinkedIn", luego en "Seguidores", decide si quieres que todos en LinkedIn sigan tus actualizaciones públicas o solo tus seguidores.

Además

- Ten cuidado con los contactos sincronizados si tienes fuentes confidenciales, y considera eliminar todos los elementos sincronizados del calendario.
- Asegúrate de no haber publicado un CV antiguo con dirección particular.
- Elimina tu escuela secundaria.

X

X es una de las plataformas que más se utilizan para acosar periodistas y es uno de los primeros lugares donde los atacantes podrían buscar vulnerabilidades en la protección de tu privacidad.

Toma medidas para bloquear su perfil, entre ellas:

- Decide si quieres usar una foto que pueda usarse en programas de reconocimiento facial para rastrearte y cuánto quieres añadir a tu biografía.
- Evita añadir tu fecha de nacimiento a tu perfil, así como tu ubicación, que también debería estar desmarcada en "Tus publicaciones".
- En el menú "Privacidad y seguridad", selecciona "Proteger tus publicaciones" en la sección "Público, contenido multimedia y etiquetado" para limitar quién puede ver tus publicaciones. Desactiva "Etiquetado de fotos".
- Decide quién puede enviarte mensajes en la sección "Mensajes directos".
- Decide si las personas que tienen tu correo electrónico o número de teléfono pueden encontrarte en "Descubrimiento".
- Ten cuidado al sincronizar los contactos de tu teléfono con X si incluyen fuentes sensibles.
- Desactiva "Anuncios personalizados" en "Preferencias de anuncios" en la sección "Compartir datos y personalización".
- Desmarca la opción para personalizar tu experiencia en "Identidad inferida" o compartir tu información con socios comerciales en "Compartir datos con socios comerciales".
- Decide si quieres que tu contenido se use para entrenar a Grok, la IA de X.

Sitios web personales

Si tienes un sitio web personal, el dominio se asociará con una dirección, un número de teléfono, un nombre y un correo electrónico. Es una forma sencilla de obtener tu información de contacto.

- Accede a DomainTools, introduce la URL de tu sitio web y comprueba si tu información personal es pública.
- Considera ocultarla con un servicio de protección de la privacidad como Who is Guard.
- Consulta con tu registrador de dominios para ver qué opciones gratuitas o de pago ofrece para ocultar la información personal.

Cambiar las contraseñas de las cuentas hackeadas

Si has sido hackeado, es posible que tu nombre de usuario y contraseña se hayan vendido y estén disponibles en la web oscura.

- El sitio web have i been pwned? te informará si tus contraseñas y nombres de usuario se han visto comprometidos en filtraciones de datos. Cambia la contraseña inmediatamente y las de otras cuentas que usen la misma combinación de nombre de usuario y contraseña.
- Usa gestores de contraseñas como Keeper Security para crear contraseñas o frases de contraseña largas y aleatorias.
- Habilita la autenticación de dos factores. Usa una aplicación de autenticación en lugar de mensajes SMS para recibir los códigos de 2FA.
- Usa una dirección de correo electrónico bien protegida, como Gmail, con una YubiKey.
- Considera crear un nombre de usuario seguro basado en una nueva cuenta de correo electrónico que solo uses para un propósito específico, por ejemplo, para acceder a portales de compras.

Intermediarios de datos

Hay docenas de intermediarios de datos que recolectan información y la compilan en informes que venden. Puedes optar por no participar, pero esto puede ser difícil y podría ser necesario hacerlo muchas veces, lo cual requiere mucho tiempo.

- Suscríbete a un servicio de exclusión automática, como DeleteMe y Optery, que se encargará de todos los trámites.
- Usa la aplicación Permission Slip para enviar solicitudes de exclusión automáticas. La versión de pago tiene más funciones.

Anexo 3. Herramientas para periodistas y responsables de la Redacción

Herramienta	Para qué se utiliza
Tall Poppy	Paquete completo de servicios de mitigación del acoso en línea, desde capacitación hasta respuesta a incidentes y servicio de conserjería para VIP
PEN America	Capacitación
Troll Busters	Capacitación y consultoría
Theseus	Análisis de amenazas
DeleteMe	Eliminación de información personal
Permission Slip app	Eliminación de información personal
Mark Monitor	Protección de marca, gestión de dominios, protección contra suplantación de identidad
Proofpoint	Protección contra suplantación de identidad
ZeroFox	Vigilancia de la web oscura, protección contra la suplantación de identidad
Elv.ai	Moderación de contenidos, vigilancia de amenazas
Memetica	Vigilancia de amenazas
Interfor	Vigilancia de redes sociales, vigilancia de amenazas
Ontic	Investigaciones y análisis de amenazas
Dataminr	Vigilancia de amenazas
JustDeleteMe	Eliminación de cuentas antiguas
TweetDelete	Eliminación de publicaciones antiguas en X
tweeteraser	Eliminación de publicaciones antiguas en X
Google's PerspectiveAPI	Moderación de comentarios

Other resources

- Manual de campo sobre acoso en línea de PEN America
- Lista de verificación de seguridad digital fácil de usar de Zebra Crossing
- Consultas de seguridad individuales de la International Women's Media Foundation
- Informe sobre el acoso en línea a periodistas de Reporteros Sin Fronteras

INSI

INTERNATIONAL
NEWS SAFETY
INSTITUTE

International News Safety Institute
C/O Thomson Reuters Foundation
5 Canada Square
Floor 8
Canary Wharf
London E14 5AQ

info@newssafety. org
www. newssafety. org
@INSInews