TOOLKIT SHOTS HEARD ROUND THE WORLD

Orientación sobre cómo prepararse, defenderse y seguir adelante después de un ataque antivacunación.

TOOLKIT SHOTS HEARD ROUND THE WORLD

En nuestro actual mundo virtual, son muchos los profesionales de la salud que comparten su experiencia en redes sociales para ayudar a que los pacientes estén bien informados. Con demasiada frecuencia, estos profesionales de la salud son acosados, intimidados y atacados.

En este kit de material, le brindaremos las habilidades y la información necesaria para **prepararse, defenderse** y **seguir adelante** después de haber sufrido un ataque antivacunación en una variedad de plataformas en línea. Esperamos capacitarlo y brindarle los recursos necesarios para continuar siendo un defensor en línea de las vacunas.

QUIÉNES SOMOS

Shots Heard Round the World (Shots Heard o SH) es una caballería digital de respuesta rápida dedicada a proteger las páginas de redes sociales de los proveedores y los consultorios de atención sanitaria.

Somos una red de respuesta rápida sin ánimos de lucro, minuciosamente examinada, y basada con total orgullo en la evidencia, que se dedica a combatir los ataques antivacunas que se producen en las páginas de redes sociales, sitios web y sitios de reseñas de proveedores, consultorios, hospitales y sistemas de salud completos. **Si defiende la ciencia de las vacunas, nosotros también lo defenderemos.**

Sabemos de primera mano que el valor que tiene este tipo de red virtual de respuesta rápida es inmenso y profundo. Vea la historia de nuestros fundadores.

Shots Heard está dirigido por personal de Public Good Projects, una organización sin ánimo de lucro dedicada a abordar los problemas de salud pública más urgentes en todo el mundo.

¿QUÉ PUEDE HACER ANTE UN ATAQUE?

PREPÁRESE Y EVITE

Existen una serie de medidas que puede tomar mientras trabaja en mejorar su presencia en línea y defiende el uso de vacunas que lo ayudarán a evitar ser atacado por antivacunas o a prepararse en caso de ser atacado.

Tenga sus refuerzos listos

- Únase a la caballería digital The Shots Heard Round The World
- Correo electrónico Join@shotsheard.org
- Únase al grupo privado de The Shots Heard Facebook Group
- Conozca la comunidad: consulte publicaciones pasadas relacionadas con el apoyo, el compañerismo y la educación

Evalúe su presencia en Internet

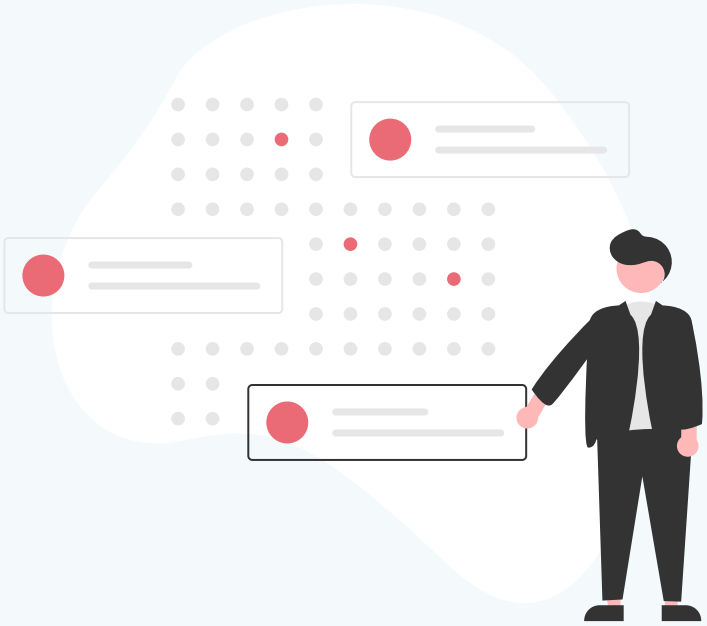
- No alimente a los trolls: para evitar más comentarios negativos, ignore aquellos comentaristas negativos, acosadores o intimidadores
- Evite discusiones innecesarias y participe con cautela: si va a participar con un comentario en contra de la vacuna, elija de manera sensata sus conversaciones según el contexto.

  A continuación, se incluyen algunos aspectos a tener en cuenta:

  - ¿La persona que comenta lo hace de buena fe? ¿Están abiertos a llevar un diálogo productivo? ¿Le están provocando?
  - ¿Conoce a esta persona o confía en ella?
  - ¿Tienen un largo historial de publicaciones antivacunas y forman parte de grupos antivacunas?

Construya una red confiable

- Los perfiles de «amigos» o «seguidores» que han mostrado un comportamiento positivo y que pueden ser aliados
- Anime a que se escriban reseñas positivas de su lugar de trabajo



Ponga a punto su lugar de trabajo, oficina y/o institución

- Teléfonos: capacite al personal para que reconozca las señales de un ataque y aprenda a responder y saber cuándo notificarlo a la dirección
  - Si sus teléfonos no dejan de recibir llamadas en tono negativo, grosero o de broma:
    - Si es posible, ignore/silencie el teléfono o apáguelo
    - Si la llamada se produce en una línea que no puede ignorar, determine si se trata de una llamada negativa y, de ser así, cuelgue o despídase cortésmente.
    - Anote el número de llamadas telefónicas fraudulentas e incluya números de teléfono y mensajes.
- Conozca las señales de un inminente ataque a través de las redes sociales
  - El personal responsable del seguimiento de las cuentas debe estar capacitado para buscar:
    - Un aumento o un volumen superior al habitual de comentarios negativos.
    - Comentarios inusualmente irrespetuosos o mezquinos de cuentas nuevas
    - Enlaces o capturas de pantalla de su página que se publican en grupos antivacunas o en páginas antivacunas
    - Personas en los comentarios de sus páginas que animan a otros antivacunas para que lo ataquen
    - Comentarios negativos provenientes de cuentas sospechosas, anónimas o de tipo bot
    - Antivacunas que contactan con usted a través de otras plataformas

Haga un seguimiento de la seguridad de su cuenta en Internet:

- Active la autenticación de dos factores para todas las cuentas que la admitan
- Utilice contraseñas seguras y diferentes o un gestor de contraseñas

Conozca la configuración de su plataforma en caso de ataque:

Sepa cómo limitar o desactivar rápidamente los comentarios, bloquear cuentas infractoras, hacer que su perfil sea privado, denunciar cuentas infractoras y eliminar comentarios ofensivos (consulte los enlaces en la sección «Defiéndase» que aparece a continuación).

Algunas tácticas preventivas que le pueden ayudar a evitar y disuadir ataques:

1. Evalúe la opción de que sus cuentas sean privadas:
   Privacidad de Instagram
   Privacidad de Twitter
   Privacidad de Tiktok
2. Promueva su negocio en Internet
   Yelp
   Google My Business
3. Habilite las notificaciones por correo electrónico: de esta manera, sabrá enseguida si se ha producido un ataque
   Notificaciones de Facebook
   Notificaciones de Yelp
   Notificaciones de Google My Business

«Googlee» y busque si está sufriendo «doxing» usted mismo

El doxing se utiliza para identificar públicamente o publicar información privada sobre un individuo o una organización, generalmente con el propósito de castigar o vengarse. Es importante saber si su información personal está disponible públicamente en Internet. En caso de que lo esté, tenga en cuenta que podrá ser más vulnerable a sufrir «doxing».

Consejos ***del New York Times***:

1. Busque usted mismo en motores de búsqueda como Google y elimine la mayor cantidad de información suya que aparezca en las diferentes fuentes.
2. Elimine su información presente en las páginas de búsqueda de personas o en las empresas de administración de datos
3. Cambie sus redes sociales a privadas

DEFIÉNDASE

Muchos profesionales de la atención sanitaria han sido atacados en Internet, especialmente después de haber compartido información veraz basada en la ciencia. Aunque puede llegar a ser frustrante, perturbador y realmente aterrador, lo superará, así como lo han hecho muchos de sus compañeros de profesión en el pasado.

Aquí tiene 10 medidas importantes que debe tomar de inmediato en caso de que sufra un ataque:

1. Recuerde: superará esta situación y no está solo.

1. Pídanos ayuda.

3. No se enzarce con los atacantes.

4. Desactive las notificaciones de las redes sociales.

5. Aumente los ajustes de privacidad de la plataforma y las páginas que han sido atacadas.

6. Realice capturas de pantalla y registre todos los ataques, incluidos los comentarios negativos, las reseñas fraudulentas y otros contenidos similares.

7. Informe y bloquee a los atacantes y elimine los comentarios negativos.

8. Promueva sus negocios en Yelp y Google.

9. Informe a su empleador/ empleados sobre la situación.

10. Tómese descansos para cuidarse corporal y mentalmente.

Medidas específicas a realizar en las plataformas:

Facebook
Aumente sus ajustes de privacidad
Deshabilite las publicaciones de visitantes
Desactive las reseñas y recomendaciones de Facebook
Denuncie publicaciones de intimidación, doxing o desinformación

Instagram
Haga que su perfil sea privado
Denuncie publicaciones de intimidación, doxing o desinformación

Twitter
Proteja sus Tweets (haga que la cuenta sea privada)
Denuncie publicaciones de intimidación, doxing o desinformación
Bloquee cuentas agresivas

Tiktok
Aumente sus controles de privacidad
Denuncie y elimine comentarios de acoso, doxing o desinformación

Yelp
Denuncie reseñas fraudulentas
Señale usuarios

Google Reviews
Denuncie reseñas fraudulentas

SIGA ADELANTE DESPUÉS DE HABER SUFRIDO UN ATAQUE

Los ataques pueden terminar de manera gradual o rápida, pero en todo caso notará como el empeño a la tendencia negativa disminuye cuando los antivacunas son bloqueados: ven limitado su radio de acción y pierden el interés. Una vez que aprecie dicha disminución, es fundamental tomarse un tiempo para descansar, limpiar sus páginas y organizarse.

- Organice todas las capturas de pantalla y registros de ataques.
- Comente las acciones tomadas con los miembros del personal, moderadores o familiares que tengan acceso a su página o hayan sido testigos del ataque. Asegúrese de reunir todas las pruebas necesarias, evaluar el acceso de cara al futuro y comprobar la salud mental de los afectados.

Medidas específicas a realizar en las plataformas:

Facebook
- Elimine las páginas sobrantes para páginas comerciales

Instagram
- Elimine comentarios negativos

Twitter
- Oculte respuestas | API de Twitter | Docs

Tiktok
- Elimine comentarios

Yelp
- Denuncie todas las reseñas de yelp fraudulentas restantes

Google Reviews
- Envíe un mensaje directo a Twitter a @Googlemybiz; explique brevemente el ataque y pida ayuda
- Repita el paso 1 según sea necesario (ya que puede ser realmente necesario)
- Intente también: Solicitar la eliminación de las reseñas - Android - Ayuda de Google My Business

QUÉ HACER SI SUFRE DOXING

Pasos específicos de las medidas a tomar:

1. Denuncie las páginas y los comentarios ofensivos que hagan referencia al sitio web o plataforma (por lo general aparece en la página/comentario una opción para «denunciar»)
2. Cambie las cuentas de sus redes sociales a privadas
3. Recabe ejemplos de doxing mediante capturas de pantalla
4. Busque su presencia en la red utilizando los motores de búsqueda (Google, Bing, Firefox, etc.) y elimine su información en las fuentes que aparece.
5. Póngase en contacto con el servicio al cliente del sitio de búsqueda de personas o con la empresa administradora de datos para eliminar su información
6. Eliminación de contenido de Google - Ayuda legal
7. Configure alertas para su nombre completo en Google: Alertas de Google: supervise la Web para encontrar nuevos contenidos interesantes
8. Busque su presencia en páginas webs con espacios para chatear como Reddit y 4Chan
9. Cambie todas las contraseñas para estar más seguro

Si el doxing se convierte en amenazas graves de violencia, póngase en contacto con las autoridades locales y el FBI Recursos:

- Globalsign.com: Cómo evitar sufrir doxing
- Berkely.edu: Protéjase ante el «doxing»
- DHS.gov: Cómo prevenir el acoso en Internet mediante «doxing»
- NYT: Guía para evitar el doxing en Internet
- NYT: Listas de verificación de seguridad y privacidad de las redes sociales
- NYT: Guía del programa de estudios sobre el doxing
- Formulario de denuncia del FBI

CUÍDESE

SALUD MENTAL

El hecho de ser atacado puede provocar que se sienta aislado. Tenga bien presente que nunca está solo y que hay esperanza y luz al final del túnel. **Gracias por el trabajo que aporta proporcionando atención médica e información objetiva en Internet.**

Busque recursos de tratamiento para la salud mental

- CDC resources para personas que buscan tratamiento
- Recursos para la prevención del suicidio: si tiene pensamientos suicidas, busque ayuda en alguna de las asociaciones locales o llame a una de las líneas directas que aparecen a continuación
- Línea de ayuda nacional para la prevención del suicidio
- Fundación Estadounidense para la Prevención del Suicidio
- Centro de Recursos para la Prevención del Suicidio
- Instituto Nacional de Salud Mental

Busque recursos en línea sobre acoso e intimidación

- Centro de investigación contra el ciberacoso: Recursos
- HeartMob de Hollaback:Conoce tus derechos

SOLIDARIDAD

Podemos ponerle en contacto con otras personas que han pasado por una situación parecida. Póngase en contacto con nosotros si está interesado.you're interested.

Historias de personas que han superado con éxito los ataques producidos a través de Internet:

- Vea nuestra historia en shotsheard.org

SEGURIDAD FÍSICA

- Si no se siente seguro en casa, mire la opción de quedarse con un amigo o familiar con quien se sienta más seguro
- Avise a los agentes de seguridad que hay en su trabajo o en el área donde vive
- Si ha recibido amenazas, llame a la línea directa (que no sea de emergencia) de la comisaría de policía de su localidad

Recursos si en el lugar donde se encuentra se siente físicamente inseguro:
Puede denunciar cualquier amenaza directa o de doxing al FBI. Encuentre su oficina local del FBI en este enlace.

DEJE DE UTILIZAR EL INTERNET SI PUEDE

Realice actividades que le hagan sentirse bien: salga a despejarse, haga ejercicio, cocine, lea, pase tiempo con las personas que ama.

Evalúe la opción de desactivar las notificaciones en **todas las cuentas de redes sociales** si de esta manera se siente seguro y cómodo.

CONOZCA LAS REGLAS

Puede ser útil conocer las leyes que existen entorno a los diferentes tipos de ataques que se producen en Internet, como el doxing y el ciberacoso, a aquellos profesionales de la salud que están expuestos a sufrir dichos ataques. Las leyes y sus aplicaciones varían de un estado a otro. Consulte la información que aparece a continuación para obtener una descripción general legal sobre este tema. Tenga en cuenta que esto no es un consejo legal y no pretende reemplazar la asistencia de un abogado.

LEYES

Identificar la necesidad de hacer cumplir la ley

- Si siente que su integridad está en peligro, llame al 911

Según el Manual contra el acoso en línea de Pen America**, es más probable que la policía pueda ayudar de alguna manera con las siguientes formas de acoso en línea:**

- Ha recibido o ha sido mencionado en amenazas directas de violencia. (Es más probable que las fuerzas del orden se tomen en serio las amenazas si estas mencionan un momento, lugar o ubicación).
- Un abusador que actúa por Internet ha publicado imágenes suyas no consensuadas y sexualmente explícitas.
- Ha sido acosado a través de comunicaciones electrónicas (ver más abajo).
- Conoce a la persona que le acosa por Internet y desea solicitar una orden de alejamiento.

En aquellos casos en los que no se tomen medidas legales inmediatas, presentar una denuncia sobre el acoso a las fuerzas del orden público puede ayudar a establecer un registro documental de cara a acciones futuras.

- Denuncie el acoso que sufre por Internet al FBI a través de este enlace
- Denuncie amenazas y delitos al FBI
- Póngase en contacto con la oficina local del FBI

Identifique cuándo necesita recibir asesoramiento legal

- Pasos para emprender acciones legales

Recursos para encontrar un abogado

- Directorio de referencia de abogados por estado

Resumen de las leyes federales más relevantes

- Resumen de la ley federal contra el acoso
- Leyes sobre el doxxing

Recursos basados en el estado

- Las leyes contra el bullying de cada estado
- Para obtener un desglose más detallado de cada estado

TÉRMINOS Y CONDICIONES DE SERVICIO/USO/ACUERDO

La mayoría de las plataformas prohíben las publicaciones y el contenido que sea considerado bullying, acoso o que suponga la revelación pública de información personal de sus usuarios.

Términos y condiciones específicas de servicio de cada plataforma

- Facebook
- Instagram
- Twitter
- TikTok
- Yelp
- YouTube
- Google Reviews

Gracias por unirse a nosotros en nuestra misión por recuperar la ciencia, proteger la salud pública y defender a los profesionales provacunas: una publicación, un tweet y una dosis a la vez.

¡Estamos aquí para ayudarle!