Diseño de sitios web para aumentar la seguridad y la privacidad de sobrevivientes

Visitar un sitio web puede dejar un rastro digital y generar riesgos de seguridad y privacidad para los/las sobrevivientes. Un riesgo principal para los/las sobrevivientes es que alguien pueda descubrir que estuvieron buscando información o ayuda en línea. Una persona abusiva, amigos/as, familiares, compañeros/as de trabajo o compañeros/as de clase podrían conocer lo que busca un/a sobreviviente en línea tanto espiando la pantalla como mirando el historial de búsqueda.

Aunque tal vez no sea posible eliminar los riesgos por completo mediante el diseño web e incluyendo contenido sobre seguridad y privacidad, usted puede aumentar la concientización de los/las sobrevivientes y brindar opciones. A continuación encontrará consejos para reducir al mínimo los riesgos de seguridad y privacidad del sitio web de su programa.

1. **Incluya una alerta de seguridad.** La alerta de seguridad debería incluir una advertencia respecto de que visitar este o cualquier otro sitio web, e incluso buscar términos como "violencia doméstica", crea un rastro digital que no se puede borrar por completo. Una alerta de seguridad debe informar a la persona sobre los riesgos y brindarle la posibilidad de decidir si desea continuar o retirarse. También debería incluir un encabezado en la parte superior de cada página web, ya que los/las sobrevivientes podrían no ingresar desde la página principal. Por ejemplo, revise el encabezado de alerta de seguridad del sitio web de la Red Nacional para Eliminar la Violencia Doméstica (NNEDV, por sus siglas en inglés) o la pestaña emergente de seguridad en el sitio web de la Línea directa de Violencia doméstica nacional.

   Información a incluir:

   1. Otras formas de buscar ayuda, como servicios de emergencia, su línea de atención o una línea informativa nacional.

2. Una opción para abandonar rápido el sitio mediante un “botón de salida rápida” (más información a continuación) o para cerrar la ventana del navegador mediante atajos del teclado, como Alt+F4 (para Windows) o Shift+Command+W (para Mac).
3. Opciones para minimizar el rastro digital mediante el uso de dispositivos más seguros y opciones de privacidad de los navegadores. Usted puede **enlazar o copiar nuestra página de seguridad en Internet** (en Inglés) e incluir un enlace para obtener información adicional sobre seguridad y privacidad en la tecnología mediante nuestra Herramienta para sobrevivientes disponible en TechSafety.org.

AVISO: no genere una falsa sensación de seguridad. Si alguna parte de su contenido web hace referencia a eliminar el rastro digital, incluya también información sobre los riesgos de los programa espía (spyware) y el control de dispositivos. Los programa espía (spyware), también llamados programas de acoso (stalkerware), controlan toda la actividad, incluidos los intentos de borrar el historial de navegación. Lea más acerca de los programa espía (spyware) y programas de acoso (stalkerware).

2. **Incluya un botón de salida rápida** que redirija al navegador web a un sitio web confiable, con contenido neutral (como al pronóstico del clima o las noticias) y que pueda cargarse rápidamente. Un botón de salida rápida no borra el sitio actual del historial de navegación, pero puede ser una opción para que un/a sobreviviente acceda a otro sitio web rápidamente si alguien entra a la habitación mientras él/ella visita su sitio.

   Otra opción es programar el botón para que, al hacer clic, lo/la redirija a varios sitios web rápidamente para ocultar su sitio web en el historial de navegación. El beneficio de esta opción es que si alguien oprime “atrás”, no irán a su sitio; lo cual agrega una barrera más de protección y privacidad. La desventaja es que tardará más en cargar y, aun así, no elimina el historial de navegación.

3. **Aumente la seguridad y la privacidad mediante opciones como "contáctenos" y "encuentre ayuda".**

    - **Utilice guías visuales claras y lenguaje simple** para dirigir a los/las sobrevivientes hacia las formas más seguras y confiables para ponerse en contacto con usted.
    - **Aliente a los/las sobrevivientes a ponerse en contacto a través de su línea directa** o mediante cualquier otra opción más segura y confiable que usted ofrezca (por ejemplo, por mensaje, chat en línea, etc.). Visite nuestro Conjunto de Herramientas de Servicios Digitales y obtenga más información si está considerando comenzar nuevos servicios.
    - **Elimine las direcciones de correo electrónico de su sitio web y utilice formularios web.** Para los/las sobrevivientes que se comunican con su programa, las líneas directas y los chat en línea son, en general, opciones más seguras para comunicarse. Sin embargo, los formularios de contacto en línea suelen ser una mejor opción para los/las sobrevivientes, en comparación con el correo electrónico. Con un formulario en línea, los mensajes de los/las sobrevivientes se envían a través de su página web en vez de enviarse a través de la cuenta de correo electrónico de los/las sobrevivientes, donde podrían encontrarse los mensajes enviados. En el formulario web, es importante incluir preguntas sobre cómo su organización puede responder de forma segura. Consulte el formulario de contacto de la Red de Seguridad Tecnológica a modo de ejemplo.[1]

    AVISO: el correo electrónico y las redes sociales no son medios normalmente seguros para comunicarse. Si bien aconsejamos que los

[1]Los formularios web también son útiles para su programa, ya que reducen la cantidad de correos electrónicos no deseados enviados automáticamente por tecnologías que recolectan correos electrónicos desde sitios web. También puede dirigir mejor las consultas de visitantes que no sean sobrevivientes, por ejemplo, de personas que deseen hacer voluntariado o que soliciten un/a orador/a experto/a.

programas respondan a los/las sobrevivientes sin importar cómo se hayan contactado, asegúrese de ofrecer otras opciones más seguras desde el diseño de su sitio web y a través del contacto con el/la sobreviviente después de que haya hecho su consulta.

4. **Utilice HTTPS.** HTTPS encripta la información compartida entre los navegadores de los/las usuarios/as y su sitio web; aun así, la visita a su sitio aparecerá en el historial de navegación. HTTPS tampoco protege contra programas espía (spyware) y los dispositivos registradores de pulsaciones. Configurar su sitio web para SSL/HTTPS conlleva el beneficio agregado de mejorar su posicionamiento en los motores de búsqueda. Solicite al hospedador de su sitio web que agregue un certificado SSL, si es que todavía no cuenta con uno.

5. **Tenga precaución con las herramientas de terceros.** A veces llamadas extensiones, *plugins*, o *widgets*, estas herramientas de terceros pueden ofrecer agregar secciones con comentarios, mapas, imágenes, el clima o demás funciones a su sitio web. Algunas de estas herramientas están diseñadas para recolectar información sobre cualquier persona que visite su sitio, lo cual puede generar un riesgo serio de privacidad.

6. **Los enlaces, que incluyen videos anexados y documentos pdf, también dejan un rastro digital.**

    - Informe a los/las sobrevivientes que los enlaces a videos externos quedarán tanto en el historial de navegación como en el historial de la cuenta. Por ejemplo, un video compartido desde YouTube quedará registrado en su historial de navegación y en el historial de visualizaciones de su cuenta de YouTube. Una alternativa es compartir el video en su propio sitio.
    - Informe a los/las sobrevivientes que descargar un pdf de su sitio guardará el documento en su carpeta de descargas.

Confidencialidad del programa

Los sitios web también pueden generar desafíos respecto de las obligaciones de confidencialidad de los programas si están configurados de forma que recolectan información personal identificable (PII, por sus siglas en inglés) de quienes visitan el sitio. Cierta información básica del sitio web, como la dirección de protocolo de Internet, puede ser personalmente identificable. Al igual que con el resto del trabajo con los/las sobrevivientes, recolecte la menor cantidad de información posible que sea necesaria para brindar la información o los servicios que soliciten. Conozca más en nuestras Herramientas de confidencialidad (en Inglés).

A continuación encontrará opciones para minimizar o eliminar la recolección de información del/de la usuario/a identificable o potencialmente identificable.

1. **No utilice *cookies*.** Las cookies son pequeños códigos que registran las visitas de los/las usuarios/as a su sitio y, en ocasiones, incluso registran el historial de otros sitios que visiten. Si su sitio utiliza cookies, explique por qué utiliza cookies en su política de privacidad.

2. **Oculte las direcciones de protocolo de Internet de los visitantes de su sitio.** Las direcciones de protocolo de Internet pueden ser personalmente identificables y suelen almacenarse por defecto en la mayoría de los sitios web. Técnicas como Cryptolog (en Inglés) mezclan la dirección de protocolo de Internet con otra información aleatoria y la encriptan, protegiendo la privacidad de los/las visitantes de su sitio.

3. **Sea selectivo respecto de sus datos analíticos.** Considere no utilizar datos analíticos de terceros. Alternativamente, utilice solo la información que pueda recolectar del registro del servidor del hospedador web. Si debe usar datos analíticos de terceros, adapte los ajustes para minimizar la posibilidad de recolectar información identificable. Informe a los/las usuarios sobre cualquier análisis de terceros que utilice y brinde información acerca de cómo los/las visitantes pueden decidir no participar del análisis en su sitio mediante la

política de privacidad. También puede utilizar una herramienta como ésta (en Inglés), que se integra a su sitio web.

4. **Obtenga consentimiento informado para los nombres, fotografías, documentos y videos que usted publique en su sitio web.** Esto incluye presentadores/as, donantes, miembros de directorio, personal, voluntarios/as y otros/as individuos/as cuya información usted publique (incluidos boletines informativos enviados por correo electrónico). Elimine cualquier contenido del cual su organización no tenga consentimiento explícito para publicarlo. Además, elimine las etiquetas geográficas (en Inglés) de los archivos digitales antes de publicar fotos en su sitio web. Las etiquetas geográficas añaden información sobre la ubicación donde se tomó la fotografía. Por ejemplo, una fotografía dentro de un albergue confidencial podría revelar la ubicación exacta si fue tomada con un dispositivo con la herramienta de etiqueta geográfica activada.

5. **Brinde información clara acerca de sus políticas de privacidad.** Debe incluir información sobre qué datos recolecta su sitio web, quién tiene acceso a la información y cómo la utiliza. Para obtener más información, consulte nuestra guía para las Políticas de Privacidad y Términos de Servicio. También pueden analizar sus políticas actuales con esta herramienta (en Inglés).

Asegure la accesibilidad

Los programas deben garantizar que todo el mundo pueda acceder a sus sitios. Lea más sobre los Consejos para comenzar con la accesibilidad web de las Iniciativas de Accesibilidad Web (en Inglés).

 Este producto fue financiado por el acuerdo de cooperación n.° 2019-V3-GX-K017, otorgado por la Oficina para Víctimas de Delito, Oficina de Programas de Justicia, Departamento de Justicia de los Estados Unidos. Las opiniones, los hallazgos, las conclusiones o las recomendaciones aquí expresados pertenecen a los/las contribuyentes y no necesariamente reflejan la postura oficial ni las políticas del Departamento de Justicia de los Estados Unidos. Actualizamos nuestro material con frecuencia. Visite TechSafety.org para obtener la última versión de este y otros materiales.