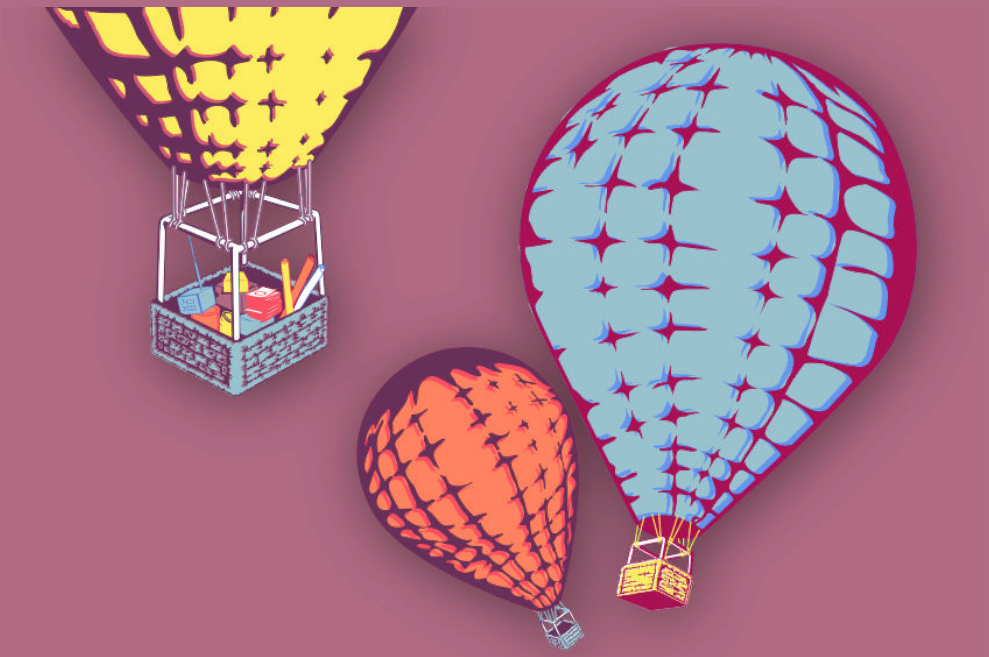
CIBERMUJERES



Activismo online más seguro

Sitios web más seguros

https://iwpr.net/

Índice general

1 Sitios web más seguros **5**
Conducir la sesión 6
Parte 1 – ¿Qué aspecto tiene un ataque online? 6
Parte 2 – Protegiendo y asegurando sitios web 7
Referencias 9

Sitios web más seguros

- **Objetivos:** Identificar prácticas más seguras para implementar y administrar nuestros sitios web, tanto sitios personales como sitios de activismo online y de nuestras organizaciones/colectivas/movimientos. recuerda que hay muchas personas y organizaciones interesadas en atacar sitios web, no sólo los/as actores que identificamos como adversario/as. existen personas que buscan sistemáticamente comprometer sitios web. independientemente si identificamos a un/a agresor/a potencial, es importante mantener un nivel alto de protección en nuestro sitio.
- **Duración:** 50 minutos
- **Formato:** Sesión
- **Habilidades:** Avanzado
- **Conocimientos requeridos:**
  - Conceptos básicos de seguridad digital y/o capacitación previa
  - Familiaridad con cómo se administran sitios web.
  - ¿En quién confías?[1]
- **Sesiones y ejercicios relacionados:**
  - ¿En quién confías?[2]

[1] https://cyber-women.com/es/ejercicios-para-fortalecer-la-confianza/en-quién-confías/
[2] https://cyber-women.com/es/ejercicios-para-fortalecer-la-confianza/en-quién-confías/

  - Apps & Plataformas online: ¿Amigo/a o enemigo/a?[3]
  - Campañas online más seguras[4]
- **Materiales requeridos:**
  - Diapositivas (con los puntos claves descritos a continuación)
  - Computadora y proyector configurados
- **Recomendaciones:** Esta sesión será más relevante para algunos grupos que otros. prioriza esta sesión especialmente para activistas y colectivos que tienen un sitio web. prepara, desde antes, ejemplos (noticias y reportajes, posts de blogs, posts en plataformas de redes sociales, experiencias personales) de ataques en línea contra sitios web de defensoras y organizaciones de defensoras. recuerda que, en algunos casos, las organizaciones no administran sus sitios o tienen limitaciones para realizar cambios, dependiendo de su estructura (ong's internacionales, por ej.) de todas maneras, aún si no pueden incidir directamente en la gestión de su web, esta sesión les brindará una base sólida para que puedan empezar a pensar sobre los cambios que puedan necesitar (o incluso tomar control sobre su propio sitio).

Conducir la sesión

Parte 1 – ¿Qué aspecto tiene un ataque online?

1. Arranca la sesión revisando algunas respuestas compartidas en la sesión de "¿En quién confías?" (Ejercicios para fortalecer la confianza) – en particular, comenta algunos de los posibles adversarios identificados por las participantes. Ésto brindará un contexto útil para abordar el tema de seguridad de sitios web, especialmente para activistas en espacios online.
2. Detona las siguientes preguntas:

[3] https://cyber-women.com/es/privacidad/apps-y-plataformas-online/

[4] https://cyber-women.com/es/activismo-online-más-seguro/campañas-online-más-seguras/

¿Qué consideran un ataque en línea?

¿Qué casos de ataques online conocen?

Si consideras oportuno, pregúntales si algún grupo o participante ha sido atacada en el pasado. También puedes compartir estudios de caso, previamente preparados para la sesión, si no surgen otros ejemplos.

3. Plantea las siguientes preguntas relacionados con los casos compartidos:

   ¿El ataque surgió en el contexto de un evento específico como una protesta, la presentación de un informe u otro tipo de encuentro?

   ¿Cuáles fueron las respuestas por parte de las defensoras involucradas?

   ¿Se documentó el caso?

Parte 2 – Protegiendo y asegurando sitios web

3. Basándonos en los ejemplos, comparte algunas recomendaciones iniciales para mejorar la protección de sus sitios. Incluimos algunos ejemplos a continuación. Según los diferentes niveles de conocimiento en el grupo, quizás quieras ofrecer explicaciones más en detalle:

   Opcional: aunque haya participantes que estén familiarizadas con el manejo de sitios web, antes de proceder a recomendaciones, es buena idea explicar de qué maneras se puede administrar un sitio web. Algunos temas a cubrir aquí pueden ser: dominios, DNS, web hosting y sistemas de manejo de contenidos (CMS).

Proteger tu sitio web

- Utiliza una contraseña de administradora robusta para evitar que comprometan tu sitio. El acceso indebido a sitios web, aprovechando contraseñas débiles, es uno de los ataques más comunes en este ámbito.

Cuando sea posible, activa la autenticación de dos factores a la administración de tu sitio, cuenta de hosting y otros portales de acceso vinculados a tu sitio web.

- Cuando registras un dominio, generalmente te piden proporcionar datos como nombre, dirección postal y correo electrónico. Comprueba qué información queda disponible para los demás en tu registro de dominio (puedes hacer ésto buscando el dominio en 'whois.net') y considera optar por un registro privado de dominio.
- ¿Dónde está alojado geográficamente el dominio? Toma en cuenta lo siguiente:
  - ¿En qué país (incluso en qué ciudades) están localizados los servidores que alojan el dominio? ¿Puedes confiar tus datos al gobierno de dicho país y, más importante aún, puedes confiar en el servicio de hosting y de dominio en que no vaya a entregar tus datos ante una solicitud gubernamental? ¿Dicho gobierno podría intentar interferir con o intentar inhabilitar tu sitio?
  - Piensa dos veces si comprar tu dominio a una empresa que revende dominios. Ante una situación de ataque, vas a querer tener comunicación con el equipo de soporte para que te puedan ayudar. Algunas empresas son notorias por dar mal soporte técnico.
- Verifica qué plugins utiliza el sitio web. Un plugin es un programa que depende de otro y le agrega nuevas funciones. Wordpress, entre otros CMS, suelen integrar plugins. Asegúrate de sólo utilizar plug-ins cuando sea necesario y verifica que las que están habilitadas procedan de una fuente de confianza.
- Analiza si es apropiado, en tu caso, utilizar Jetpack (de Automatic) en tu Wordpress, especialmente para servicios como los widgets de plataformas de redes sociales y formularios de contacto. Existen plugins para hacer respaldos básicos de tu sitio como Better WP Security. Otros realizan respaldos automáticos como Vault Press o Backup Buddy.
- Procura actualizar con frecuencia tu CMS, plugins y las demás plataformas que estás administrando. Si tu servicio de hosting no realiza

mantenimiento, asegúrate de cubrir ese aspecto directamente o a través de terceros de confianza.

Proteger las personas que navegan tu sitio

- Es altamente recomendable que tu sitio web ofrezca una conexión HTTPS por defecto (y no opcionalmente). Lets Encrypt de Electronic Frontier Foundation es un servicio que expide y verifica certificados de manera gratuita.
- Existen muchos colectivos en todas las latitudes que, desde las trincheras de las tecnologías, apoyan y se especializan en trabajar con organizaciones activistas. En Latinoamérica existen, por ejemplo, los proyectos Código Sur y Kefir.red. Otros colectivos afines son Autistici, NoBlogs y Blackblogs.org.
- Si alguna plataforma u sitio de una organización/colectivo/proyecto social sufre un ataque de denegación de servicio (DDOS), considera usar servicios como Deflect o Project Shield. Deflect es un proyecto de la organización sin ánimo de lucro, basada en Montreal, Equalit.ie. Ofrecen un servicio gratuito de mitigación de DDOS, avalado por la comunidad de seguridad digital.
- Investiga los plug-ins antes de instalarlos. ¿Qué reputación tienen las personas desarrolladoras? ¿Ha sido auditada (revisión de código)?¿Ofrecen soporte técnico? No instales algo sólo porque esté de moda.

Opcional: considera compartir información sobre cómo responder ante un ataque de DDoS. Ej: https://github.com/OpenInternet/MyWebsiteIsDown/blob/dev/MyWebsiteIsDown.md

Referencias

- https://onlinesafety.feministfrequency.com/es/

- https://www.apc.org/es
- https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/es