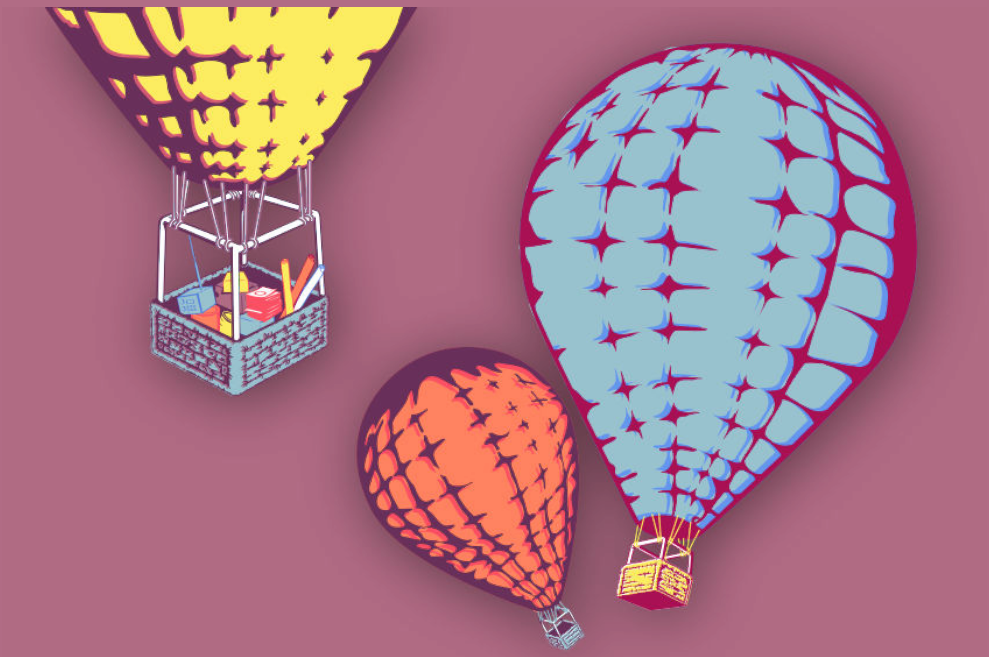
CIBERMUJERES



Activismo online más seguro

Activismo online más seguro

https://iwpr.net/

Índice general

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

Campañas online más seguras

- **Objetivos:** Compartir recomendaciones de seguridad digital para defensoras de derechos humanos que están involucradas en esfuerzos de campañas online.
- **Duración:** 50 minutos
- **Formato:** Sesión
- **Habilidades:** Intermedio
- **Conocimientos requeridos:**
  - ¿En quién confías?[1]
- **Sesiones y ejercicios relacionados:**
  - ¿En quién confías?[2]
  - Modelo de riesgos con perspectiva de género[3]
  - Apps & Plataformas online: ¿Amigo/a o enemigo/a?[4]
  - Modelo de riesgos con perspectiva de género[5]

[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/

[3] https://cyber-women.com/es/buscando-la-mejor-solución/modelo-de-riesgos-con-perspectiva-de-genero/

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

[5] https://cyber-women.com/es/buscando-la-mejor-solución/modelo-de-riesgos-con-perspectiva-de-genero/

  - Sitios web más seguros[6]
  - Creando contraseñas más seguras[7]
  - Malware y virus[8]
  - Cómo hacer más segura tu computadora[9]
- **Materiales requeridos:**
  - Diapositivas (con los puntos claves descritos a continuación)
  - Computadora y proyector configurados
- **Recomendaciones:** La intención de esta sesión es que las participantes identifiquen soluciones de seguridad digital con el fin de implementar prácticas más seguras a la hora de hacer campañas online; sin embargo, el objetivo final no es que las lleven a cabo durante la sesión, sino que empiecen el proceso de exploración de qué es más apropiado para sus contextos individuales.

Esta sesión se basa en la guía desarrollada por Indira Cornelio para SocialTIC.

Conducir la sesión:

Parte 1 – Introducción y planeación en prevención

1. Aclara a las participantes que la intención de esta sesión es que identifiquen soluciones de seguridad digital con el fin de implementar prácticas más seguras a la hora de hacer campañas online. No tendrán que implementarlas inmediatamente sino empezar a explorar cuáles son las más apropiadas para sus contextos y campañas.
2. Pídeles que compartan ejemplos de campañas online que conozcan. En su opinión, ¿existen tendencias emergentes?

[6] https://cyber-women.com/es/activismo-online-más-seguro/sitios-web-más-seguros/

[7] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/creando-contrasenas-más-seguras/

[8] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/malware-y-virus/

[9] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/cómo-hacer-más-segura-tu-computadora/

3. Subraya que, a la hora de armar su campaña y hacer activismo en internet, deberían tomar en cuenta la información y lo/as adversario/as que identificaron durante la sesión de "¿En quién confías?". Las campañas, por ser esfuerzos llevadas a cabo en la esfera pública, implican prestar especial atención a quiénes podrían estarlas potencialmente monitoreando y amenazando en general.

4. Sugiéreles que, cuando se trata de arrancar con la fase de planeación de campaña en sus contextos de trabajo y acción, pueden trabajar en grupos las siguientes preguntas:

    - ¿De qué trata la campaña?
    - ¿A qué público se dirigen? ¿Cómo se sienten/cuál es su postura con respecto al tema que están tratando? ¿Están a favor o en contra?
    - ¿Quiénes podrían sentirse expuestas o blanco de un ataque en esta campaña?
    - ¿Cuáles podrían ser los argumentos potenciales que podrían formular contra la campaña?
    - ¿Cuáles serían los mejores y peores resultados de esta campaña?

5. Responder estas preguntas puede ayudar a planear de manera más estratégica medidas preventivas ante posibles amenazas. Enfatiza que pueden hasta preparar mensajes respuesta por anticipado, tomando en cuenta posibles escenarios que pueden emerger. Los posibles escenarios positivos también pueden implicar planear medidas preventivas: por ejemplo, ¿cómo podrían prepararse ante la posibilidad que, si la campaña es un éxito y se vuelve muy conocida, su sitio web no pueda manejar tantas visitas y colapse?

6. Aclara que durante los siguientes pasos de la sesión, estarás brindando orientaciones y recomendaciones sobre prácticas de seguridad digital útiles para campañas online (si tienen tiempo, visiten sitios web de algunas herramientas).

Parte 2 – Proteger dispositivos

7. Pregúntales a las participantes si usan sus dispositivos personales para hacer sus campañas (vs. un dispositivo destinado específicamente a su "trabajo"). En caso afirmativo, ¿cuánta información relacionada con la campaña almacenan ahí? ¿Están conectadas, en el mismo dispositivo, a sus cuentas de correo y plataformas de redes sociales?

8. Algunas prácticas recomendables a destacar en este sentido son:

    - Poner contraseña a sus computadoras y celulares.
    - Instalar un programa de antivirus en sus computadoras y celulares.
    - Respaldar regularmente datos importantes y confidenciales (registros de video, audio, anotaciones de entrevistas, informes, etc.) y guardar estos respaldos en lugares seguros que no estén cerca de sus dispositivos.
    - Habilitar el cifrado completo de sus dispositivos:
        - En caso de dispositivos móviles Android y Mac iOS, pueden habilitar esta función en la configuración del celular.
        - Para computadoras: Filevault para Mac OSX[10] y BitLocker para Windows[11] son opciones comunes.

Aclaración: Filevault está ya instalado en Mac OSX sin coste adicional; sin embargo, BitLocker sólo viene de manera gratuita en Windows versión Pro, Enterprise y Education.

Parte 3 – Administrando accesos a tus cuentas

9. Las campañas online suelen requerir que varias personas accedan a una misma cuenta (o dispositivo, en algunos casos). Y ésto aumenta los posibles riesgos. Sin embargo, tomando algunas medidas preventivas, puedes reducir significativamente la probabilidad de que estos riesgos se traduzcan en amenazas:

[10] https://es.wikipedia.org/wiki/FileVault
[11] https://es.wikipedia.org/wiki/BitLocker

- Para todas estas cuentas y dispositivos compartidos, limitar al máximo la cantidad de personas que tengan acceso es una de las primeras medidas críticas a implementar; otra medida es asegurarse que se sigan, de manera regular y consistente, los protocolos y procedimientos acordados (especialmente tomando en cuenta las recomendaciones a continuación).
- Particularmente en el caso de plataformas online, todas las personas que tengan acceso deberían verificar regularmente el historial y actividad de dichas cuentas. Por ejemplo, en cuentas de Gmail/Google, pueden verificar el historial de inicios de sesión recientes (y establecer alertas para actividades con patrones sospechosos) bajo la opción de "Última actividad de la cuenta"; de la misma manera, en Facebook, pueden ir al "Historial de actividad" bajo la opción de "Actividad reciente".
- Aplica prácticas básicas de contraseñas robustas para todos los dispositivos y cuentas que se van a utilizar en la campaña. Los administradores seguros de contraseñas como Keepass/KeepassX (http://keepass.info/) permiten crear bases de datos de contraseñas de cuentas. Esta base de datos se accede a través de una contraseña maestra. También recomendamos habilitar la autenticación de dos factores en Google, Facebook y Twitter para sumar una capa adicional de control de acceso.
- Si tienen que compartir una contraseña entre diferentes personas del grupo y no lo pueden hacer en persona, hazlo a través de opciones seguras como correo cifrado - con GPG o un servicio como Tutanota (https://tutanota.com/)- o chat cifrado (con la app Signal para celulares). Si utilizas Signal, asegúrate de establecer un protocolo de borrar historiales de chat o mensajes donde aparezcan estas contraseñas lo antes posible después de recibir la información requerida.

Parte 4 – Escoger apps para campañas

10. A la hora de implementar y organizar una campaña online, se acostumbra a utilizar determinadas apps y herramientas para monitorear las estadísticas de plataformas de redes sociales y sitios web; también para programar publicaciones. A la hora de escoger estas apps y tomar decisiones sobre ellas, tomen en cuenta las siguientes preguntas para evitar compartir información confidencial a través de herramientas inseguras o que ya no son mantenidas por el equipo desarrollador:

    - ¿Esta app está siendo actualizada regularmente (funcionalidades, aspectos de seguridad, etc)?
    - ¿El equipo desarrollador o el proyecto tiene cuentas en plataformas sociales para darle seguimiento e interactuar?
    - ¿Qué dicen los demás sobre esta app?
    - ¿Tienen blog? ¿Hay publicaciones recientes?

Parte 5 – Desarrollo comunitario a través de Facebook

11. Facebook es comúnmente utilizado en campañas online para organizar comunidades y difundir de manera rápida. Sin embargo, es importante subrayar algunas vulnerabilidades potenciales que emergen al utilizar estas plataformas como herramienta central de la campaña:

    - Recomendamos que las participantes vayan tomando conciencia sobre las implicaciones que tiene usar Facebook (u otras plataformas de redes sociales hegemónicas) en su manejo de identidades en línea. Con el fin de limitar qué tanto se exponen, pueden crear perfiles específicos para administrar las páginas de su campaña y organización/colectivo/proyecto en vez de usar sus perfiles personales. Toma en cuenta que ahora puedes recibir notificaciones cifradas (con tu llave pública de GPG asociada a tu cuenta de correo) de Facebook. Esto puede ser útil para defensoras que quieren tomar más medidas a la hora de separar sus identidades.

- Es altamente recomendable que reflexionen sobre qué tipos de información y comunicaciones comparten. Existen ejemplos de páginas y perfiles de campañas en Facebook que han sido infiltradas por adversario/as, obligando a las administradoras a cerrarlas; y también casos donde Facebook ha cerrado estas páginas y perfiles por denuncias de terceros.
- Enfrentarse a una situación de censura puede ser un contratiempo significativo por lo que es importante contar con canales alternativos de organización y comunicación como:
- Generar simultáneamente comunidades activas en otras plataformas para que siempre haya un alternativa/respaldo ante una contingencia; Descarga la información de las páginas y los perfiles de la campaña en Facebook;
- Usa listas de correos de Riseup[12] para enviar boletines y otra información; Organiza reuniones cara a cara cuando sea posible aunque, según el contexto, puede ser una opción arriesgada y poco aconsejable.

Parte 6 – Consentimiento informado

12. Discute la importancia del consentimiento informado, especialmente relevante en casos de campañas de concientización en derechos humanos donde se utilizan testimonios de víctimas, sobrevivientes y personas testigo de violencia y violaciones.

    Antes de registrar imágenes o videos de estas personas o documentar sus historias, debes pedir de antemano consentimiento explícito, para el registro en sí y para la difusión pública posterior. Informa a las personas para qué van a utilizar estos contenidos y cuáles son las posibles implicaciones de ello.

[12] https://riseup.net/es/lists

Referencias

- http://seguridadigital.org/post/156287966318/consejos-de-seguridad-digital-para-gestionar-redes
- https://archive.informationactivism.org/es/index.html

¿Qué dicen tus metadatos sobre ti?

- **Objetivos:** Introducir el concepto de metadatos y la importancia de tomar conciencia sobre qué metadatos contiene cada tipo de contenidos, especialmente cuando estamos trabajando en situaciones de riesgo en el ámbito de derechos humanos.
- **Duración:** 90 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - Multitudes interconectadas[1]
  - Campañas online más seguras[2]
- **Materiales requeridos:**
  - Diapositivas (con los puntos claves descritos a continuación)

[1] https://cyber-women.com/es/privacidad/multitudes-interconectadas/

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

  - Computadora y proyector configurados
  - Ejemplos de herramientas para analizar y eliminar metadatos
- **Recomendaciones:** Aunque no es necesario, esta sesión se puede aprovechar más si las participantes ya han repasado la sesión "multitudes interconectadas". el tema de los metadatos es uno de los más complejos de presentar en los talleres de capacitación. dedica suficiente tiempo a cubrir esta sesión en detalle ya que es bastante crítico y relevante en el contexto de defensoras y mujeres activistas.

Conducir la sesión

Parte 1 - ¿Qué son los metadatos?

1. Arranca la sesión compartiendo algunos puntos clave:
   - Comparte una definición de metadatos y dónde pueden encontrarlos comúnmente: imágenes, archivos Word y Excel, etc.
   - Comparte algunos ejemplos típicos de metadatos (fecha, hora, ubicación donde el archivo fue creado, nombre de usuario/a o autor/a, tipo de dispositivo). Pueden verificar los metadatos de un archivo de su computadora o compartir capturas de pantallas de los metadatos que aparecen en los formatos de archivos más conocidos.
   - Explica varias maneras en que se crean los metadatos y cómo pueden ser modificados/eliminados.

   El tema de los metadatos es uno de los más complejos de presentar en los talleres de capacitación, así que asegúrate de preguntar si quedó clara la explicación y, si no fuera así, resolver dudas en profundidad.

Parte 2 - Implicaciones de metadatos en el contexto de derechos humanos

2. A la hora de trabajar con defensoras, es importante explicar las ventajas y desventajas de los metadatos. Puedes hacerlo a través de dos ideas clave:

   Los metadatos pueden revelar mucho sobre ti.

   - Tomen una foto con sus celulares y verifiquen todos los metadatos que contiene la imagen. Muéstrales la app CameraV y la herramienta web Metapicz (http://metapicz.com).
   - Ahora vuelvan a tomar una foto, pero esta vez con la función de ubicación desactivada en sus celulares. Divide las participantes en grupos de 3 o 4 (máximo) para que discutan en qué sentidos creen que los metadatos pueden ser útiles y cómo pueden comprometer la seguridad de las personas que trabajan en derechos humanos.
   - En la discusión grupal, mantén el enfoque en el trabajo de derechos humanos. Es importante que puedan identificar en qué circunstancias los metadatos contenidos en documentos, videos e imágenes puedan servir como evidencia a la hora de documentar casos de derechos humanos. Comparte algunas prácticas como guardar archivos originales en dispositivos cifrados y crear copias separadas para edición y almacenamiento en otras computadoras.

   Los metadatos se crean, pero también pueden ser eliminados.

   - Comparte varias opciones para borrar metadatos en videos e imágenes como ObscuraCam y Metanull. Si tienen suficiente tiempo, pueden probar eliminar los metadatos de documentos a través de LibreOffice.

Referencias

- https://ssd.eff.org/es/module/por-qu%C3%A9-los-metadatos-son-importantes
- https://guardianproject.info/apps/obscuracam/ (Sin referencia en español)
- https://es.witness.org/recursos
- https://securityinabox.org/en/lgbti-mena/remove-metadata/ (Sin referencia en español)