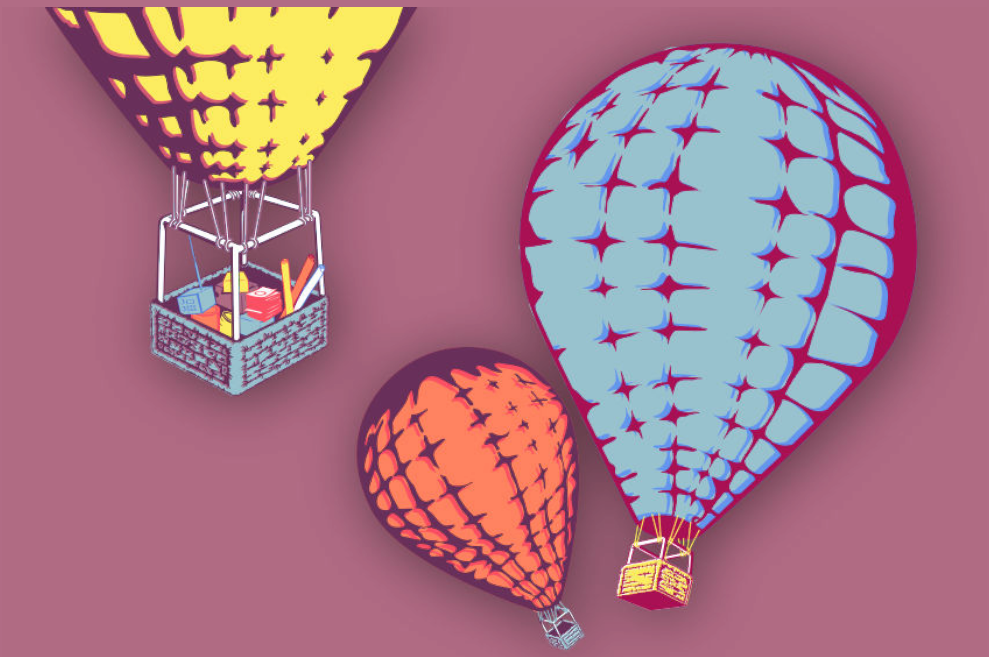
CIBERMUJERES



Activismo online más seguro

Campañas online más seguras

https://iwpr.net/

Índice general

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