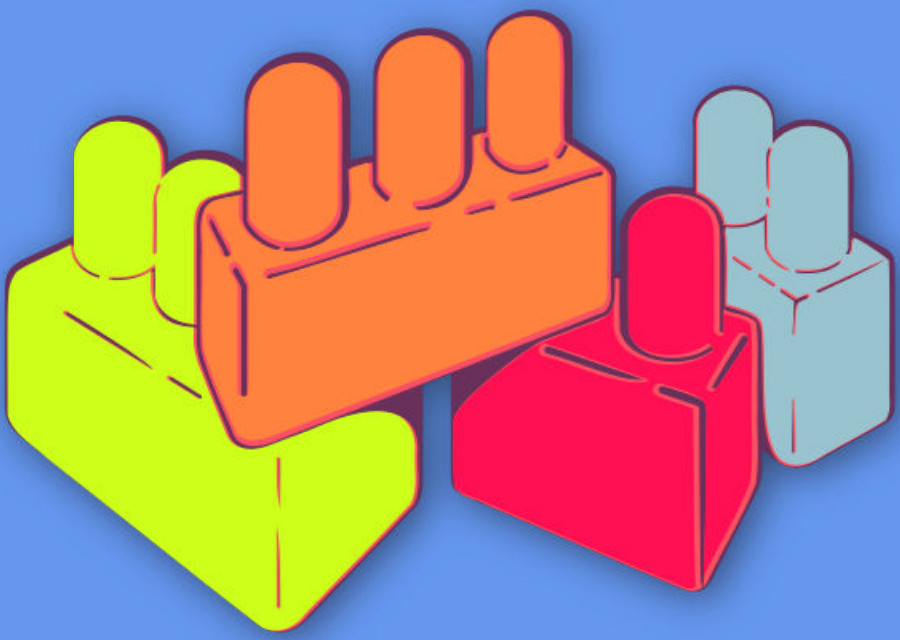
CIBERMUJERES



Principios básicos de seguridad digital 1

Malware y virus

https://iwpr.net/

Índice general

Malware y virus

- **Objetivos:** Abordar, en un contexto de riesgos cercano a las realidades de las defensoras, conceptos básicos de malware y la exposición de nuestros dispositivos a distintos tipos de malware y software malicioso.
- **Duración:** 30 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - ¿Cómo funciona Internet?[1]
  - Cómo hacer más segura tu computadora[2]
- **Materiales requeridos:**
  - Diapositivas (con los puntos claves descritos a continuación)
  - Computadora y proyector configurados
- **Recomendaciones:** Idealmente, después de esta sesión, sigan con la de

[1] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/cómo-funciona-internet/

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

"cómo hacer más segura tu computadora", también incluida en este módulo.

Conducir la sesión

Parte 1 - Introducción al Malware

1. Explica a las participantes qué es el malware, un repaso de algunos tipos - como mínimo, recomendamos cubrir los siguientes:

    - Troyanos
    - Spyware
    - Ransomware
    - Keylogger (registrador de teclas)
    - Virus

    El ransomware y los registradores de teclado (keyloggers) son tipos de malware cada vez más comunes en el contexto de las defensoras en Latinoamérica; si estás trabajando con un grupo de mujeres en esta región, será especialmente importante abordarlas. En general, asegúrate de incluir estudios de caso y ejemplos de malware que sean comunes en las realidades de las participantes de tu taller.

Parte 2 - ¿Cómo te puedes infectar?

2. Explica algunas de las maneras más comunes de infección de malware. También es importante explicar los distintos propósitos o motivaciones que puede tener el uso de malware:

    - Algunos se viralizan a una escala amplia sin ningún objetivo concreto.
    - Otros van dirigidos específicamente a activistas, periodistas o disidentes para obtener acceso a sus datos y comunicaciones.

- O a personas que están en contacto con una red de activistas y defensoras y que, a través de infectar su equipo, alcancen el resto de su red.

Parte 3 - Comparte ejemplos que afecten a mujeres y defensoras de derechos humanos

3. Concluye la sesión compartiendo ejemplos de casos de infección de malware comunes en el contexto de mujeres y defensoras; puedes basarte en estudios de caso (de blogs, portales de noticias o desde la experiencia personal de cada una). Recuerda anonimizar las fuentes al menos que tengas permiso explícito de la(s) persona(s) afectada(s). Aquí mostramos algunos ejemplos de casos. Quizás conozcas casos similares más relevantes a tu contexto.

   > Una mujer que recibió un correo que oferta boletos gratuitos a un concierto; el enlace que contenía el correo infectó su smartphone (celular inteligente) con malware.
   >
   > Una activista recibió un correo de quien era, aparentemente, un/a compañero/a; al hacer clic en el enlace del correo, un mensaje aparece diciendo que su disco duro está cifrado y que necesita pagar para obtener acceso de vuelta a sus datos.

Referencias

- https://securityinabox.org/es/guide/malware/
- https://ssd.eff.org/es/module/protegi%C3%A9ndote-contra-el-malware