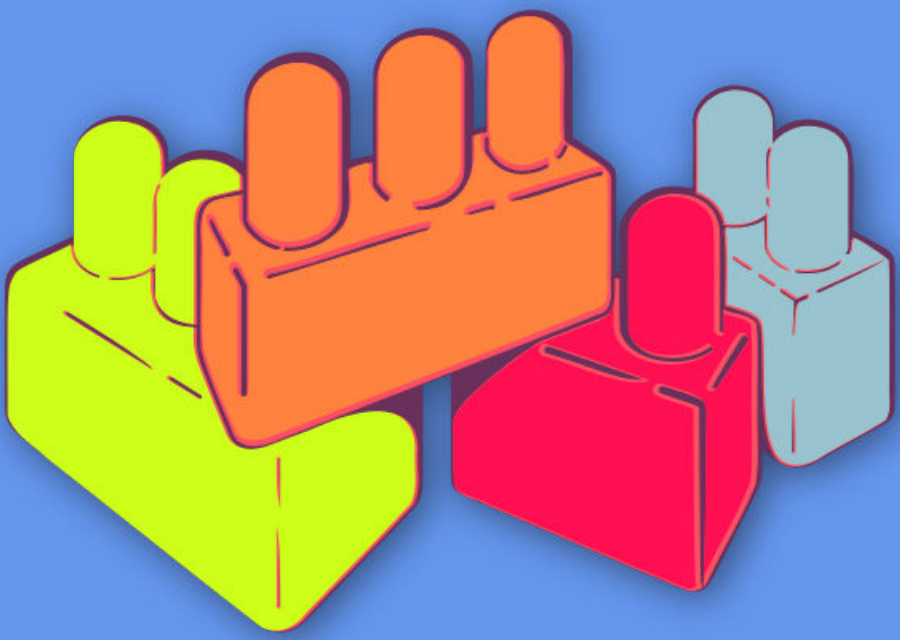
CIBERMUJERES



Principios básicos de seguridad digital 1

¿Cómo funciona Internet?

https://iwpr.net/

Índice general

¿Cómo funciona Internet?

- **Objetivos:** Compartir una comprensión de los flujos de información de internet, las distintas vulnerabilidades que emergen y buenas prácticas de seguridad relacionadas a cada componente y tramo de la cadena.
- **Duración:** 60 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - ¿En quién confías?[1]
  - Impresiones personales sobre la seguridad[2]
  - Nuestros derechos, nuestra tecnología[3]
- **Materiales requeridos:**
  - ¿Cómo funciona Internet? Tarjetas de representaciones icónicas

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

[2] https://cyber-women.com/es/repensar-nuestra-relación-con-las-tecnologías/impresiones-personales-sobre-la-seguridad/

[3] https://cyber-women.com/es/repensar-nuestra-relación-con-las-tecnologías/nuestros-derechos-nuestra-tecnología/

de los distintos componentes de la ruta que sigue un correo electrónico desde que se envía hasta que es recibido: dispositivos (computadora/celular) (x 2) (nota: representa la computadora y el celular en la misma tarjeta para evitar confusiones), módem (x2), poste telefónico/fibra óptica subterránea (x 2), proveedor de servicio de Internet (x 2), servidores Google (x 1), simulacro de email (x 2, o más)
  - Documentos con sugerencias sobre prácticas de seguridad digital
  - Papel para utilizar a modo de pizarrón: un trozo de 4 metros y dos trozos de 1 metro cada uno.
  - Marcadores de colores
  - Cinta adhesiva
  - Diapositivas (con puntos clave comentados a continuación)
  - Computadora y proyector ya configurados
  - Altavoces/bocinas
- **Recomendaciones:** Procura cubrir todas las preguntas que puedan surgir. es importante cerrar la sesión cubriendo las inquietudes que puedan surgir en torno a las vulnerabilidades comentadas en la sesión y que sientan que tienen la información necesaria para tomar medidas. evita crear un entorno de miedo, estrés o ansiedad - brinda suficiente información y recursos, además de señalar otras oportunidades para formación (si es posible).

Esta sesión fue desarrollado conjuntamente con Mariel García (SocialTIC) y Spyros Monastiriotis (Tactical Technology Collective)

Conducir la sesión:

Parte 1 - Cómo funciona Internet – Flujos de información y puntos de vulnerabilidad.

1. Esta parte del taller comenzará a modo de juego. Cada participante recibe tarjetas representando diferentes componentes de una cadena de flujo de información (módem, computadora, edificio de proveedor de servicio de internet, etc.). Pide a las participantes que las ordenen correctamente para mostrar cómo se envía un correo a través de Internet.
2. Haz observaciones del orden de las tarjetas y repasa el proceso con el grupo. Pide a una persona voluntaria que explique el proceso de nuevo en sus propias palabras. Recomendamos pedir que tres personas en total cuenten el proceso de vuelta. Puedes cambiar las ilustraciones de referencia y en qué orden se explica para darle más variedad al ejercicio. Procura un tiempo para resolver dudas también.
3. Puedes apoyarte en un recurso audiovisual como https://www.youtube.com/watch?v=7_LPdttKXPc para ayudar a las participantes a identificar si están ordenadas correctamente las tarjetas.

   Opcional: para grupos más grandes, en vez de una tarjeta por persona, reparte una por pareja; para grupos más pequeños, coloca todas las tarjetas en el suelo y debate en grupo el orden.

Parte 2 - Vulnerabilidades

4. Una vez completado el paso anterior, las participantes colocan cada tarjeta en un papel grande en el suelo. Repasa de nuevo la cadena, esta vez señalando y explicando las vulnerabilidades en cada etapa (comparte brevemente algunas buenas prácticas relevantes para generar una sensación de calma y confianza entre las participantes)

Comentaremos algunas vulnerabilidades a continuación. Puedes agregar otras prácticas o vulnerabilidades que consideres relevantes a tu propio contexto o los contextos de las participantes. También puedes compartir algunos ejemplos de prácticas de otros colectivos con los que trabajas, con el fin de ayudar a las participantes pensar cuáles podrían ser prácticas buenas o malas en su caso.

Dispositivo 1 (computadora/celular): inseguridad física; pérdida de información

Módem 1: sniffing de WiFi; información sin cifrar

Poste telefónico/fibra óptica subterránea: no aplica

Proveedor de servicio de internet: solicitudes de datos y metadatos de instancias gubernamentales locales/nacionales

Servidores de Google: vigilancia internacional; contraseñas inseguras y phishing, solicitudes de instancias gubernamentales nacionales

Poste telefónico/fibra óptica subterránea 2: N/A

Módem 2: problemas de seguridad al utilizar las conexiones de terceros (ej. cibercafé)

Dispositivo 2: software malicioso; borrado inseguro de datos

Parte 3 - Buenas prácticas de seguridad digital

5. Una vez que se hayan centrado en las vulnerabilidades, para que no sea demasiada información para las participantes que tienen menos experiencia en estos temas, cada grupo tomará un papel que describa una posible solución. Este papel será el detonante para discutir en grupo.

   Al final, los grupos tendrán entre 30 segundos y un minuto para presentar sus ideas (una de las facilitadoras tomará notas y aportará retroalimentación). Las facilitadoras se moverán por el espacio dando explicaciones cortas y respondiendo preguntas y, sobre todo, alentando la discusión entre las participantes.

Es importante que, conforme avance esta actividad, las facilitadoras expliquen los conceptos básicos de cada solución. También, según el nivel de interacción y ritmo del taller, quizás no dé para cubrir todas las propuestas.

Algunas de las más importantes para tomar en consideración son:

Inseguridad física: reduce la exposición de los dispositivos de tu organización a personas desconocidas.

Inseguridad física: utiliza bloqueos de dispositivos en tu oficina y casa.

Pérdida de información: guarda tu respaldo en un lugar que no sea tu oficina o casa.

Pérdida de información: escoge una persona para encargarse de los respaldos en tu organización.

Intevención de redes (WiFi sniffing): retira todas las indicaciones que muestren la contraseña de WiFi.

Intervención de redes (WiFi sniffing): cambia la contraseña de tu WiFi frecuentemente.

Datos sin cifrar: asómate a una criptofiesta en tu ciudad o participa en un taller.

Datos sin cifrar: lee la sección sobre cifrado del manual "Security in a Box".

Solicitudes de datos y metadatos por parte de entidades gubernamentales locales/nacionales: trabaja con organizaciones de derechos digitales para encontrar maneras para protegerte legalmente.

Solicitudes de datos y metadatos por parte de entidades gubernamentales locales/nacionales: investiga qué dicen las leyes en tu país sobre la intervención de comunicaciones.

Vigilancia internacional: cámbiate a servicios seguros para realizar búsquedas, administrar tu correo, alojar tus datos y comunicaciones en general.

Contraseñas inseguras: utiliza contraseñas largas y complejas.

Contraseñas inseguras: utiliza KeePass para recordar todas las contraseñas que tienes.

Phishing: piensa antes de hacer clic (presta atención donde introduces tus datos de acceso a una cuenta).

Utilizar el WiFi de otras personas: siempre cierra adecuadamente tu sesión.

Utilizar el WiFi de otras personas: cuéntanos -¿qué no deberías estar revisando cuando estás en el WiFi de otra persona?

Software malicioso: instala un programa de antivirus y ejecútalo manualmente cada semana.

Borrar datos de manera segura: usa Cmd+derecha para vaciar la papelera en Mac.

Borrar datos de manera segura: utiliza programas como Eraser o CCleaner.

Parte 4 - Asuntos y recursos pendientes

6. Este momento de la sesión es para sondear preguntas relacionadas con seguridad digital que no hayan surgido en el taller hasta ahora, además de discutir temas relevantes en las comunidades de las participantes. Aprovecha para compartir materiales para seguir aprendiendo y mantenerse al día. La facilitadora hará ronda de preguntas, dará unas pistas de posibles respuestas y mencionará referencias que pueden servir para responderlas más en profundidad.

Referencias

- https://securityinabox.org/es
- https://ssd.eff.org/es

- https://myshadow.org/es
- http://www.sinmiedo.com.co
- https://cuidatuinfo.org
- https://temboinalinha.org
- https://prism-break.org/es