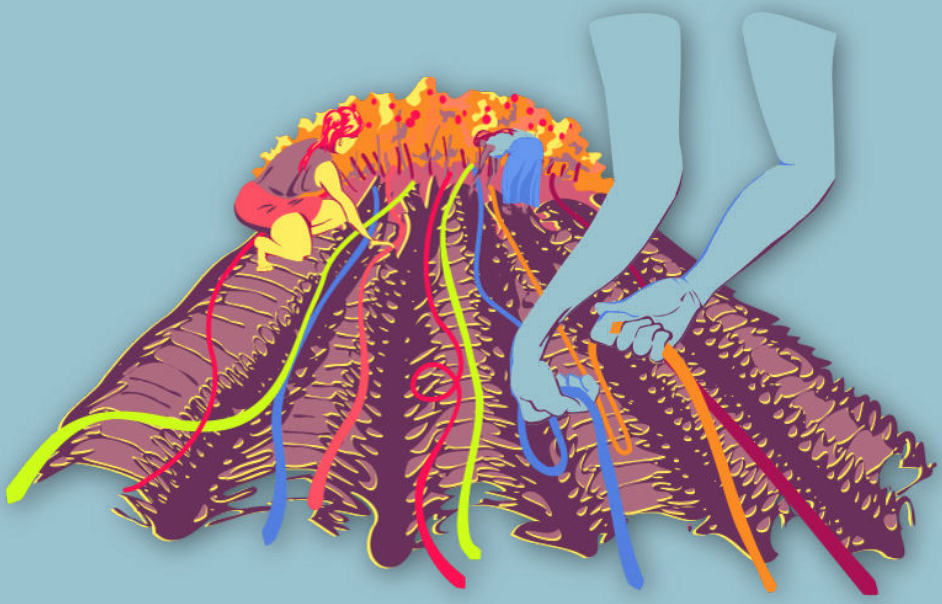
CIBERMUJERES



Buscando la mejor solución

Toma de decisiones sobre seguridad digital

https://iwpr.net/

Índice general

Toma de decisiones sobre seguridad digital

- **Objetivos:** Introducir el proceso de pensamiento crítico estratégico necesario para tomar decisiones fundamentadas a la hora de implementar prácticas y herramientas de seguridad digital. identificar recursos que puede ayudarlas a mantenerse al día después de la capacitación.
- **Duración:** 90 minutos
- **Formato:** Sesión
- **Habilidades:** Intermedio
- **Conocimientos requeridos:**
  - Conceptos básicos de seguridad digital y/o capacitación previa.
- **Sesiones y ejercicios relacionados:**
  - Impresiones personales sobre la seguridad[1]
  - ¿En quién confías?[2]
  - ¿Cómo funciona Internet?[3]

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

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

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

  - Apps & Plataformas online: ¿Amigo/a o enemigo/a?[4]
- **Materiales requeridos:**
  - Diapositivas (con los puntos claves descritos a continuación)
  - Computadora y proyector configurados
  - Copias impresas de infográficos de casos de defensoras (Véase Apéndice)
- **Recomendaciones:** Puesto que esta sesión requiere un nivel básico de conocimiento de partida sobre conceptos de seguridad digital, es ideal llevarla a cabo en el contexto de una capacitación de varios días o parte de un taller corto que se centra en diseñar protocolos individuales de seguridad.

Conducir la sesión

Parte 1 - Introducción

1. Arranca preguntándole a las participantes cuántas veces han preguntado a un tallerista, facilitadora o experta algo sobre seguridad digital y les han respondido de manera diferente cada vez. Un poco confuso, ¿verdad? A veces, cuando pedimos consejo sobre seguridad digital, no necesariamente implica que nos vayan a acompañar en el proceso sino sólo "arreglar el problema" en nuestros dispositivos sin explicarnos lo que hicieron. ¿Preferirías saber para poder replicar el proceso después si vuelve a surgir el problema?
2. El objetivo de esta sesión es introducir el proceso de pensamiento crítico estratégico necesario para tomar decisiones fundamentadas a la hora de implementar prácticas y herramientas de seguridad digital e identificar recursos que nos pueden ayudar a mantenernos al día después de la capacitación. Conversen sobre cómo la seguridad digital es más que descargar unas apps nuevas sino que es un proceso de conocer nuestras prácticas más de cerca y tomar decisiones con fundamento

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

con el fin de construir entornos más seguros para nosotras mismas.

Parte 2 – ¿Cómo desarrollaron el software que utilizas?

3. Muestra de nuevo herramientas y plataformas que quizás ya hayas presentado como Signal, HTTPS Everywhere, ObscuraCam, Skype, Telegram, etc. Identifiquen qué tipo de software es en cada caso. Pueden entrar en los sitios web para obtener más contexto.
4. Explica qué es el software propietario (código cerrado): ¿cuáles son las características de este tipo de software? Brinda ejemplos. ¿Cuáles son las implicaciones, a nivel de seguridad digital, al utilizar este tipo de software?
5. Explica qué es el software open source: ¿cuáles son las características de este tipo de software? Brinda ejemplos. ¿Cuáles son las implicaciones, a nivel de seguridad digital, al utilizar este tipo de software? Asegúrate de introducir qué es la comunidad de software opensource y la auditoría de código.
6. Explica qué significa FLOSS (Free/Libre and Open Source Software) : ¿cuáles son las características de este tipo de software? Brinda ejemplos. ¿Cuáles son las implicaciones, a nivel de seguridad digital, al utilizar este tipo de software?

Parte 3 – Tomando en cuenta a las usuarias

7. Si ya cubrieron la sesión ¿En quién confías? del módulo "Repensando nuestra relación con las tecnologías", repasa ejemplos de adversario/as. Si ya cubrieron la sesión de Modelo de riesgos con perspectiva de género, revisa de nuevo el modelo que crearon juntas.

   Este repaso sirve para reforzar la idea de que no todo el mundo tiene las mismas necesidades o enfrenta los mismos riesgos en materia de seguridad digital.

- Cuando estamos buscando respuestas en estos temas, sondea lo máximo posible sobre las necesidades específicas que vayas identificando. ¿Qué quieres hacer o asegurar? ¿Cuál es el lugar más seguro donde guardas algo? ¿De quién lo estás protegiendo?
- Piensa en las plataformas y herramientas que utilizas. ¿Qué tan dispuesta o qué tan posible es para ti cambiarlas por otras alternativas o cambiar tu manera en que interactúas con ellas?
- ¿Hasta qué punto te afecta tu acceso a internet a la hora de crear posibles respuestas de seguridad digital? ¿Sueles tener una conexión estable y confiable de internet o te tienes que adaptar a trabajar sin conectividad durante largos periodos de tiempo?
- Si estás considerando crear estrategias de seguridad digital para una organización o colectivo, toma en cuenta los diferentes dispositivos y sistemas operativos que las personas en el grupo están utilizando. ¿La estrategia va a poder aplicarse a todo el mundo? ¿O para la mayoría?

Parte 4 – Pensando en herramientas

8. Las siguientes preguntas son importantes a la hora de considerar nuevas plataformas o herramientas. No tienes que repasarlas ni contestarlas todas (ya que son muy específicas), pero procura leerlas en voz alta y dar un poco de contexto de por qué son relevantes:
    - ¿Es software libre o open source?
    - ¿Conoces quién lo desarrolló y/o financió?
    - ¿Está disponible en mi idioma?
    - Busca referencias en internet. ¿Qué información encontraste?
    - ¿Cuándo fue actualizado por última vez?
    - ¿Existe una versión estable disponible?
    - ¿Hay un canal de soporte?
    - ¿Qué tan fácil es de configurar?
    - ¿Ha sido testeado o auditado?

- ¿Está disponible para tu sistema operativo?
- Verifica los Términos de Servicio. ¿Estás de acuerdo con ellos o hay algo que te levanta sospecha?
- Si la herramienta o plataforma utiliza servidores remotos, ¿sabes dónde están ubicados?
- ¿Sabes si las personas desarrolladoras han entregado datos de usuarias ante una petición de una entidad gubernamental?
- ¿Cómo almacenan la información en sus servidores? ¿Está cifrada? ¿Las personas del proyecto pueden descifrar y acceder a la información?

9. Subraya de nuevo que no existe una respuesta o recomendación universal en materia de seguridad digital. Ninguna herramienta se adapta al contexto de todas. Ser estratégica a la hora de manejar herramientas y prácticas de seguridad digital tiene más que ver con conocernos mejor como usuarias y, a partir de ahí, escoger herramientas que se ajustan mejor a nuestros conocimientos y circunstancias.

10. Señala que existe mucho software de seguridad digital que implementa el cifrado en diferentes niveles. Explica la relevancia de que este tipo de software sea open source (es decir, que su código sea disponible). El software open source puede ser revisado por la comunidad para asegurar que no tiene puertas traseras; si no es una prioridad para ti que implemente cifrado, entonces puede ser que este criterio sea menos relevante (aunque puede ser ventajoso de todas maneras, por ejemplo, en términos monetarios).

11. Las participantes se dividen en grupos de 3-4 personas (máximo) y hacen una lista de todas las herramientas de seguridad digital que conocen. Responderán a las preguntas del punto 8. Cada grupo tiene 10 a 15 minutos para discutir las ventajas y desventajas de cada herramienta enumerada. Al final, compartirán lo reflexionado al resto de los grupos.

Parte 5 – Practicar a pensar en respuestas

12. Distribuye a los grupos los infográficos de casos de defensoras de derechos humanos (véase Apéndice). Asegúrate, antes de la sesión, tener suficientes para repartir. No les reveles posibles soluciones ahora. La idea es que los grupos piensen por su cuenta cuáles son posibles respuestas que se pueden llevar a cabo basándose en lo que llevan aprendido hasta ahora.

Parte 6 – Materiales para mantenerse al día

13. Es importante que las participantes tengan acceso a materiales complementarios después de la capacitación para que puedan remitir a ellos y mantenerse al día con herramientas y prácticas de seguridad digital.

    Aquí recomendamos algunos:

    - Zen y el arte de que la tecnología trabaje para ti (Tactical Technology Collective)[5]
    - Security in a Box (Frontline Defenders & Tactical Technology Collective)[6]
    - Autoprotección Digital Contra La Vigilancia (Electronic Frontier Foundation)[7]
    - Genios de Internet (Español) (Karisma Foundation)[8]

    Opcional: pueden listar diferentes organizaciones que siguen (online, en Twitter, etc.) para obtener información sobre seguridad digital en contextos locales.

[5] https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/es
[6] https://securityinabox.org/es
[7] https://ssd.eff.org/es/module/eligiendo-tus-herramientas
[8] https://karisma.org.co/genios-de-internet-una-guia-para-mejorar-tu-seguridad-en-la-red

Referencias

- https://www.seguridad.unam.mx