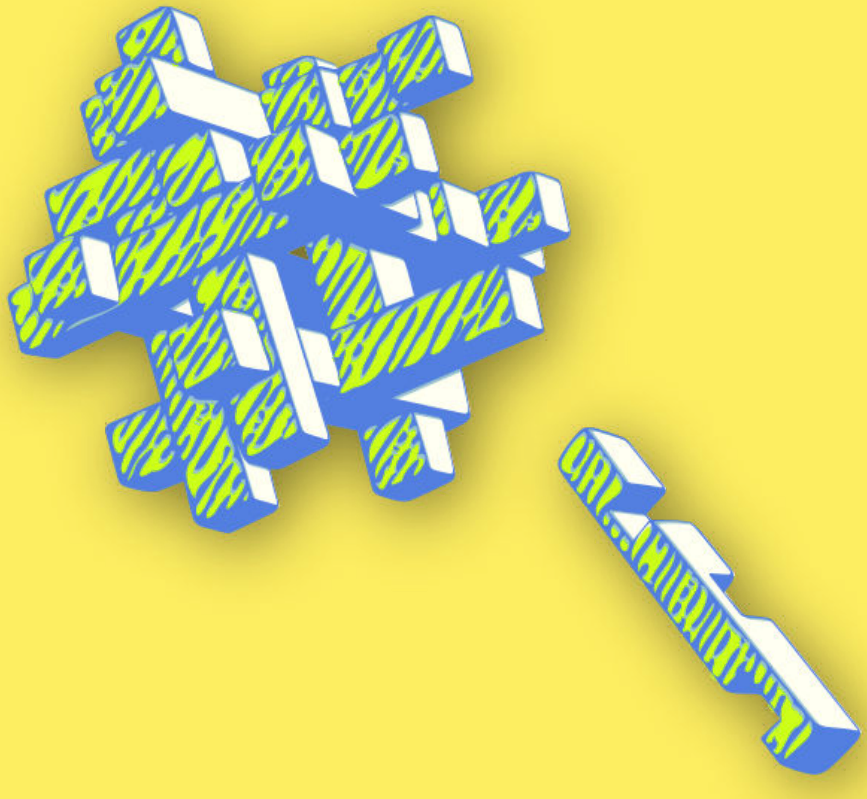
CIBERMUJERES



Cifrado

Comunicaciones cifradas

https://iwpr.net/

Índice general

Comunicaciones cifradas

- **Objetivos:** Partiendo de los contenidos formativos anteriores sobre cifrado, en esta sesión se transmite la importancia y utilidad de cifrar comunicaciones y se brindan herramientas relevantes.
- **Duración:** 50 minutos
- **Formato:** Sesión
- **Habilidades:** Intermedio
- **Conocimientos requeridos:**
  - Conceptos básicos de seguridad digital y/o capacitación previa.
  - Introducción al cifrado[1]
- **Sesiones y ejercicios relacionados:**
  - Introducción al cifrado[2]
  - Privacidad[3]
  - Campañas online más seguras[4]
- **Materiales requeridos:**
  - Diapositivas (con los puntos claves descritos a continuación)

[1] https://cyber-women.com/es/cifrado/introducción-al-cifrado/

[2] https://cyber-women.com/es/cifrado/introducción-al-cifrado/

[3] https://cyber-women.com/es/privacidad/privacidad/

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

- Computadora y proyector configurados

Conducir la sesión

1. Comparte ejemplos relevantes de situaciones donde la comunicación cifrada es útil y dedica tiempo a explicar cómo funciona el cifrado. Muestra capturas de pantalla de correos cifrados con GPG para ilustrar por encima qué aspecto tienen los mensajes y correos cuando están cifrados. También destaca implementaciones conocidas de cifrado
    - en particular, HTTPS, cifrado de punta a punta y cifrado GPG/PGP.
2. Centra la discusión en herramientas que permiten cifrar comunicaciones. Ejemplos buenos son: Signal para llamadas y mensajes, meet.jit.si para llamadas de video, Tutanota o GPG+Thunderbird para correos.
3. Explica los beneficios a nivel de seguridad de estas herramientas, sobre todo, cómo permiten a las usuarias limitar el acceso que otras personas tienen sobre sus comunicaciones; después discute situaciones donde la seguridad de los datos de la usuaria podrían ser comprometidas, aún estando cifradas. Pregunta: ¿cómo podría comprometerse un correo cifrado con GPG a través de registradores de teclas o malware que captura la pantalla? ¿Y si un/a adversario/a consigue nuestra llave privada de GPG? ¿Cómo podrían acceder a nuestros datos?
4. Si tienen tiempo, pónganse manos a la obra con al menos dos de las herramientas comentadas en el paso 2. Aunque no tengan tiempo para repasar GPG/PGP para email, pueden optar por mostrar cómo hacer llamadas de video cifradas vía HTTPS a través de meet.jit.si o instalar Signal en los celulares para practicar enviar mensajes cifrados entre sí o realizar llamadas cifradas.

Referencias

- https://ssd.eff.org/es/module/c%C3%B3mo-utilizar-signal-en-ios