CIBERMUJERES

Privacidad

Privacidad

https://iwpr.net/

Índice general

¡Pregúntame cualquier cosa!

- **Objetivos:** Explicar cómo nuestros conceptos de privacidad cambian radicalmente en los espacios online.
- **Duración:** 15 minutos
- **Formato:** Ejercicio
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - Privacidad[1]
  - Apps & Plataformas online: ¿Amigo/a o enemigo/a?[2]
- **Materiales requeridos:**
  - Diapositivas o tarjetas con preguntas (véase a continuación)
  - Diapositivas
  - Papel
  - Conexión a Internet/WiFi para descargar KeePass
- **Recomendaciones:** Es importante que compartas las indicaciones poco a poco conforme avance el ejercicio. sigue el orden descrito a continuación. si das todas las orientaciones al principio antes de arrancar con

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

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

el ejercicio, ¡revelarás la sorpresa! pregunta si se sienten en confianza hablando con el resto del grupo.

Esta sesión está basada en el módulo desarrollado por Elis Monroy del colectivo Subversiones para el proyecto Voces de Mujeres.

Conducir la sesión

1. Las participantes escogen una pareja y buscan un lugar tranquilo para conversar.
2. Las preguntas detonantes son:

- ¿Qué es la cosa más divertida o vergonzosa que te ha pasado?
- Comenta algo que detestas.
- ¿Tienes algún placer musical secreto?
- ¿Tenías un apodo de pequeña?
- ¿Quién es la persona más importante de tu vida?

Desde tu rol de facilitadora, puedes agregar o cambiar estas preguntas como veas necesario. El objetivo es romper el hielo: que emerjan anécdotas e información, quizás un poco vergonzosas o divertidas, para luego dar pie a hablar sobre la privacidad con el grupo. Puedes plantear más preguntas personales, siempre y cuando tengas en cuenta el contexto. Trata de no incomodar a las participantes.

3. Ahora se junta una pareja con otra. En total serán 4.
4. Cada participante presenta las respuestas de su pareja al otro par.
5. El grupo de 4 se junta con otro grupo de 4. Vuelven a repetir el proceso.
6. Pregúntale a las participantes cómo se sintieron en el ejercicio. Algunos temas que pueden haber salido son:

    - Quizás algunas compartieron algo porque ya conocían a su compañera y se sentían cómodas aunque no anticipaban cómo iba a cambiar la dinámica.

- Una pareja presentó de una manera distorsionada a su compañera.

7. Termina la actividad hablando sobre la privacidad y cómo algunas personas aceptan los Términos de Servicio de una plataforma sin tener claridad de cómo son "las reglas del juego" y cómo van a cambiar a lo largo del tiempo. Aborda el tema de "consentimiento" y cómo una persona puede, a veces, aceptar que le tomen una foto, pero no expresó su acuerdo (consentimiento) a que esa foto se pudiera compartir online o con otras personas.

Referencias

- https://labs.rs/en
- https://www.digitale-gesellschaft.ch/dr.html
- https://es-es.facebook.com/privacy/explanation

Privacidad

- **Objetivos:** Introducir el concepto de privacidad e identificar información sobre nosotras mismas que está en internet.
- **Duración:** 50 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - Nuestros derechos, nuestra tecnología[1]
  - ¡Pregúntame cualquier cosa![2]
  - Apps & Plataformas online: ¿Amigo/a o enemigo/a?[3]
  - Multitudes interconectadas[4]
  - Hagamos doxxing al troll[5]
- **Materiales requeridos:**

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

[2] https://cyber-women.com/es/privacidad/pregúntame-cualquier-cosa/

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

[4] https://cyber-women.com/es/privacidad/multitudes-interconectadas/

[5] https://cyber-women.com/es/violencia-en-línea-contra-las-mujeres/hagamos-doxxing-al-troll/

  - Diapositivas (con los puntos claves descritos a continuación)
  - Computadora y proyector configurados
- **Recomendaciones:** Algunas participantes pueden sentirse incómodas o disgustadas con la información pública que encuentren sobre ellas mismas en internet en el ejercicio de "auto-doxeo" de esta sesión. si esto ocurre, asegúrate de dedicar suficiente tiempo al final de la sesión para crear estrategias de respuesta. las participantes deben tener acceso a un dispositivo con conexión a internet para la parte práctica de la sesión.

Esta sesión incluye información de la sección "Auto-doxeo y recuperar el control" del manual "Zen y el arte de que la tecnología trabaje para ti" del colectivo Tactical Tech.

Conducir la sesión

Parte 1 – ¿Realmente tenemos privacidad?

1. Inicia la conversación preguntándole al grupo si creen que existe la privacidad real. Después pregúntales qué es la privacidad para ellas. Comparte tu perspectiva a modo de ejemplo. Subraya que la intención del ejercicio es que vayan reclamando su derecho a la privacidad.
2. Pídeles compartir algunos ejemplos de factores que podrían estar interfiriendo en el control que tienen sobre sus datos, información personal y otros elementos. Podrían estar relacionados con prácticas personales, las plataformas a las que confían su información, el conocimiento que tienen sobre las herramientas y dispositivos que utilizan o las acciones de los demás en sus redes.

Parte 2 – "Auto-doxeo"

3. Explica a las participantes qué significa "Doxxing": en pocas palabras, es la práctica de obtener una gran cantidad de información personal sobre alguien y hacerla pública (generalmente en línea). Puntualiza que a veces el doxxing se utiliza contra personas como táctica de venganza y, generalmente, se emplea para poner en peligro, acosar o amenazar a activistas y defensoras.
4. En esta parte de la sesión, practicarán el "auto-doxeo" como una manera de averiguar cuánto (y qué tipo de) información podemos encontrar sobre nosotras mismas online. Aclara que es un método preventivo a la hora de reducir la cantidad disponible de información (siempre que sea posible).
5. Las participantes abren un documento de texto en blanco en sus computadoras o anotan en un trozo de papel. También inician su navegador web - utilicen un navegador distinto al que acostumbran utilizar- para que no inicie sesión automáticamente en sus cuentas.
6. Antes de comenzar a navegar, cada participante crea una lista de todas sus cuentas públicas y perfiles en plataformas de redes sociales; después, anota palabras clave o frases que pueden estar asociadas a ellas, incluyendo información como:
    - La ciudad donde nacieron
    - La ciudad donde viven
    - Su dirección postal
    - La organización en la que trabajan (o con las que colaboran regularmente)
    - Sus áreas de acción en sus activismos
    - Proyectos y campañas principales en las que participan/trabajan
7. Para empezar su auto-doxeo, primero deberán buscar sus cuentas y perfiles online (deberían poder ver este cuentas/perfiles como aparecerían para el público general ya que no están con sesión iniciada en sus cuentas) y tomar nota de qué información encuentran sobre si mis-

mas.

8. A continuación, buscan sus nombres y otras palabras clave de la lista que crearon antes, utilizando el buscador de Google, DuckDuckGo, Facebook, Twitter y otras plataformas. Recomendamos algunas cuestiones más para este paso:

    - Para Google y DuckDuckGo, pueden hacer búsquedas de imágenes y vídeos, aparte de búsquedas de texto.
    - Si conocen determinadas bases de datos online - para ciudades, gobiernos, etc. - donde podrían aparecer sus datos, pueden realizar estas búsquedas ahí también.
    - Si tienen un sitio web propio, pueden buscar la url en https://whois-search.com para averiguar qué información aparece sobre ellas en el registro público de dominios.

Parte 3 – ¿Y ahora qué hacemos?

9. Explica al grupo que, a través de su auto-doxeo, quizás encuentren información sobre ellas que no sabían que estaba disponible públicamente, incluyendo cuentas que ya no utilizan y ni se acordaban que tenían.

10. Pídeles que revisen sus anotaciones y piensen qué pasos podrían seguir para tomar más control sobre lo que otras personas pueden encontrar sobre ellas en internet. Pueden realizar una lista de tareas de estos pasos que puede incluir acciones como cerrar determinadas cuentas, editar su información y/o configuraciones de privacidad de sus cuentas de plataformas de redes sociales, activar la opción de registro privado de dominio en su hosting de dominio, etc.

11. Conforme vayan haciendo estas listas de tareas, comparte algunos recursos útiles para ayudarlas a implementar algunos de estos pasos.

Herramienta de bloqueo temporal de URL: Sirve para bloquear resultados de búsquedas de sitios. No elimina el contenido, pero bloquea, hasta que se actualicen en los sitio(s) fuente, resultados de búsqueda de contenido antiguos que pueden ser potencialmente confidenciales : https://support.google

.com/webmasters/answer/1663419?hl=en&lr=all&rd=2

Eliminar cuentas de Facebook: Contiene indicaciones de cómo eliminar o deshabilitar perfiles de Facebook: https://www.facebook.com/help/250563911970368?helpref=hc_global_nav

Eliminar cuentas de Twitter: Contiene indicaciones de cómo eliminar o deshabilitar perfiles de Twitter: https://support.twitter.com/articles/15358#

AccountKiller: Instrucciones para eliminar cuentas y perfiles públicos de sitios y plataformas de redes sociales conocidas: https://www.accountkiller.com

Just Delete Me: Directorio de enlaces directos a la opción de eliminar cuentas de los servicios web y plataformas de redes sociales: http://justdelete.me

12. A modo de cierre de sesión, recuerda a las participantes que el doxeo revela información que está públicamente disponible sobre ellas; sin embargo, las plataformas de redes sociales y servicios online pueden acceder a mucha más información que esto. Subraya que pueden afianzar su seguridad utilizando contraseñas más robustas, adoptando prácticas más seguras de navegación online y utilizando cifrado para asegurar sus datos.

Referencias

- https://derechosdigitales.org/anonimato

Multitudes interconectadas

- **Objetivos:** Introducir el concepto de "multitudes interconectadas" para comprender mejor los aspectos clave e implicaciones de del papel, cada vez más protagonista, que juega la tecnología en la sociedad.
- **Duración:** 20 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - ¡Pregúntame cualquier cosa![1]
  - Privacidad[2]
  - Hagamos doxxing al troll[3]
  - ¿Qué dicen tus metadatos sobre ti?[4]
- **Materiales requeridos:**

[1] https://cyber-women.com/es/privacidad/pregúntame-cualquier-cosa/

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

[3] https://cyber-women.com/es/violencia-en-línea-contra-las-mujeres/hagamos-doxxing-al-troll/

[4] https://cyber-women.com/es/activismo-online-más-seguro/qué-dicen-tus-metadatos-sobre-ti/

  - Diapositivas (con los puntos claves descritos a continuación)
  - Computadora y proyector configurados
- **Recomendaciones:** Algunas participantes pueden sentirse incómodas o disgustadas con la información pública que encuentren sobre ellas mismas en internet en el ejercicio de "auto-doxeo" de esta sesión. si esto ocurre, asegúrate de dedicar suficiente tiempo al final de la sesión para crear estrategias de respuesta. las participantes deben tener acceso a un dispositivo con conexión a internet para la parte práctica de la sesión.

Esta sesión se basa en la investigación de Danah Boyd.

Conducir la sesión:

1. Aclara que la sesión se centra en comprender mejor qué sucede cuando la tecnología se vuelve un componente cada vez más central y esencial de la sociedad y el impacto que tiene sobre la identidad y privacidad.
2. Para ilustrar esto, presenta conceptos clave que emergen en la investigación de Danah Boyd "Taken Out of Context American Teen Sociality in Networked Publics" (La sociabilidad adolescente fuera de contexto en multitudes interconectadas).

    Multitudes interconectadas: Son, simultáneamente, el espacio construído a través de tecnologías en red y el imaginario de comunidad que emerge como resultado de la intersección entre personas, tecnología y praxis.

    Contenido de multitudes interconectadas: Inherentemente constituido por bits, que son la unidad básica de la información digital. Tanto las auto-expresiones y las interacciones entre personas producen contenido de bits en multitudes interconectadas.

    Cuatro características de las multitudes interconectadas: Las características de los bits configuran las cuatro carac-

terísticas claves de las multitudes interconectadas:

Persistencia: las expresiones online son registradas y archivadas automáticamente. Replicabilidad: los contenidos generados por los bits pueden ser duplicados. Escalabilidad: la visibilidad potencial de los contenidos es extendida. Buscabilidad: los contenidos pueden ser accedidos a través de búsquedas.

Estas cuatro características estructuran las multitudes interconectadas y las interacciones que transcurren en ellas.

Dinámicas de multitudes interconectadas: Audiencias invisibles: no todos los públicos son visibles cuando una persona contribuye online, ni están presentes a la vez > necesariamente. Contextos anidados: la falta de fronteras espaciales, sociales y temporales hace difícil mantener contextos sociales separados. Lo público y privado desdibujado: sin control sobre el contexto, lo público y privado se torna un binario sin sentido, toma dimensiones nuevas y difícilmente pueden separarse.

3. Explica y brinda ejemplos de cada una de estas características. Será útil que muestres ejemplos visuales.

Referencias

- https://es.wikipedia.org/wiki/Bits

Apps & Plataformas online: ¿Amigo/a o enemigo/a?

- **Objetivos:** Identificar los tipos de información que compartimos con las apps y plataformas online que más utilizamos, diseñar estrategias y tácticas para utilizarlas de manera segura en nuestras ámbito personal y activismo online.
- **Duración:** 120 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Principios básicos de seguridad digital y/o capacitación previa
  - Impresiones personales sobre la seguridad[1]
  - ¿Cómo funciona Internet?[2]
- **Sesiones y ejercicios relacionados:**
  - ¡Pregúntame cualquier cosa![3]

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

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

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

  - Privacidad[4]
  - Multitudes interconectadas[5]
  - Campañas online más seguras[6]
- **Materiales requeridos:**
  - Diapositivas (con los puntos claves descritos a continuación)
  - Computadora y proyector configurados
  - Papel (varias hojas por participante)
  - Post-its (de varios colores)
- **Recomendaciones:** Recomendamos que cada participante tenga acceso a internet desde su celular o algún otro dispositivo. comparte materiales complementarios donde puedan aprender más sobre la privacidad en general y pasos que puedan tomar para afianzar su propia privacidad (véase sección de "referencias" para enlaces).

Conducir la sesión:

Parte 1 – Nuestros dispositivos, nuestros datos

1. Las participantes revisarán todas las apps que tengan en sus dispositivos y verificarán lo siguiente:
   - ¿Quiénes son las personas que desarrollaron cada app?
   - ¿Cuáles tienen habilitada la función de geolocalización?
   - ¿Cuáles de las empresas propietarias de las apps podrían colaborar con las entidades gubernamentales locales?
2. Las participantes tienen 15 minutos para contestar. El grupo pone en común sus respuestas. Asegúrate de cubrir temas como los siguientes:
   - Permisos de apps que no parecen tener una relación clara con las funciones que se supone que tienen.

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

[5] https://cyber-women.com/es/privacidad/multitudes-interconectadas/

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

- Términos de Servicios que son poco claras o ambiguas.
- Políticas de Privacidad que permiten a las empresas vender los datos de las usuarias a otras empresas o instancias no declaradas claramente.

3. Comparte ejemplos de apps de menstruación ("menstruapps") - apps que ayudan a monitorear el ciclo menstrual - y otras apps relacionas con la salud personal. Explica que, según investigaciones como las de Chupadatos[7], se muestra que las menstruapps pueden recolectar bastante información personal sobre sus usuarias:

    - Nombre, número de teléfono y dirección.
    - Detalles sobre nuestro cuerpo como dolores menstruales, peso, horas de sueño.
    - Estados emocionales como estrés, falta de concentración o ansiedad.
    - Detalles sobre nuestra salud sexual, incluyendo métodos anticonceptivos.
    - Comportamientos online como los clicks que damos y los tipos de dispositivos que utilizamos.
    - Comportamientos offline como los medicamentos que tomamos o nuestros hábitos (tomar alcohol, fumar, etc.).

    Es mucha información, ¿verdad?

Parte 2 - ¿Quién más nos está rastreando?

4. Divide las participantes en grupos de 3-4 (máximo) y pide a cada grupo que hagan una lista sobre qué saben de Facebook y Google. Pueden usar las siguientes preguntas como ayuda:

    - ¿Cuál es la misión y los objetivos de estas empresas?
    - ¿Qué servicios ofrecen?
    - ¿Son servicios gratuitos o de pago?

[7] https://chupadados.codingrights.org/es/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros/

- ¿Cuáles son las condiciones y términos de estos servicios?

Tienen 15 minutos para enumerar toda la información que se les ocurre.

5. Ahora anotan en otra lista qué creen que puede saber Facebook y Google sobre ellas. Si tienen acceso a Internet, las que tienen cuenta de Google pueden entrar en https://accounts.google.com/signin/v2/identifier?service=friendview&passive=1209600&hl=es&gl&continue=https%3A%2F%2Fwww.google.com%2Fmaps%2Ftimeline&flowName=GlifWebSignIn&flowEntry=ServiceLogin para obtener más pistas. Tienen 20-25 minutos para hacer las listas. Después las presentarán al resto del grupo.

Parte 3 – Promover los derechos de las mujeres a través de plataformas de redes sociales

6. Las participantes permanecerán en los grupos de la actividad anterior. Cada grupo recibirá una serie de preguntas a discutir y trabajar juntas:

    - ¿Qué herramientas y plataformas online utilizamos para organizar e intercambiar información de nuestros movimientos sociales, protestas y campañas? ¿Cuáles son algunas de las ventajas y desventajas de utilizar estas herramientas para estos propósitos?
    - ¿Conoces ejemplos de censura de campañas y páginas en Facebook, videos en Youtube o cuentas de plataformas de redes sociales?
    - Empresas como Facebook y Google son aliadas de los gobiernos y notorias por compartir información sobre sus usuarias. ¿Qué implicaciones tiene este hecho? https://govtrequests.facebook.com (sin referencia en español).
    - ¿Conoces casos de violencia en línea contra mujeres? Específicamente, casos de amenazas en línea contra defensoras, difusión sin su consentimiento de desnudos o la creación de cuentas

falsas en plataformas de redes sociales para desacreditarlas o "anunciar" servicios sexuales en su nombre, por ejemplo ¿En qué plataformas sucedió ésto y cómo reaccionó la empresa?

Los grupos tienen 10-15 minutos para contestar las preguntas. A continuación, se pone en común las respuestas de cada grupo.

7. Dedica 5-10 minutos en reflexionar sobre cómo estas mismas plataformas de redes sociales constituyen espacios de encuentro en internet. En este sentido, son escenarios ideales para implementar esfuerzos de campañas sociales. En última instancia, Facebook y los distintos servicios ofrecidos por Google brinda diferentes maneras útiles de interactuar con las seguidoras e integrantes de nuestras comunidad en línea; por lo tanto, a pesar de los aspectos preocupantes y desventajas que puedan emerger, es importante recordar que muchas de las participantes querrán seguir utilizándolas para acercarse a sus audiencias.

Parte 4 – Reclamar nuestra privacidad

8. Facilita el cierre de esta sesión. Veremos diferentes maneras de reclamar el derecho a la privacidad en línea y adoptar una manera más segura de utilizar las apps, plataformas de redes sociales digitales, tanto a nivel personal como en nuestros activismos.
9. Permaneciendo en los mismos grupos, ahora las participantes se centrarán en crear juntas una tormenta de ideas de maneras de reclamar su privacidad. Entrega a cada grupo una serie de post-its, marcadores y lapiceros/plumas. Tienen 10-15 minutos para anotar todo lo que se les ocurra. Puedes dar ejemplos de tácticas para arrancar como:
    - Confundir a los algoritmos que las plataformas utilizan para mostrarte publicidad u optimizar contenidos.
    - Verificar con frecuencia las políticas de privacidad y las actualizaciones de las configuraciones de privacidad de las plataformas.

- Prestar atención a los permisos otorgados a nuestros dispositivos, específicamente las configuraciones de geolocalización y ubicación de nuestras fotos y posts.
- Utilizar plataformas alternativas que están más comprometidas a respetar nuestra privacidad y activismo (Riseup, Tutanota, Signal, etc.).

Los grupos tendrán la oportunidad de compartir sus ideas. Puedes anotarlas en un lugar visible de la sala para que las participantes puedan volver a ellas a lo largo del taller. Estas ideas también serán útiles conforme vayas ajustando el contenido de tu capacitación, especialmente si las participantes quieren centrarse en usar de manera más segura las plataformas de redes sociales para su activismo.

Referencias

- https://www.kaspersky.es/blog/digital-detox-advices/6226
- https://rankingdigitalrights.org/2017/08/30/rdr-en-espanol-guest-post
- https://myshadow.org/es
- https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual
- https://www.digitale-gesellschaft.ch/dr.html
- http://www.europe-v-facebook.org/ES/Objetivos/objetivos.html