CIBERMUJERES

Violencia en línea contra las mujeres

Violencia en línea contra las mujeres

https://iwpr.net/

Índice general

Esprectograma

- **Objetivos:** Este ejercicio brinda una manera útil para que las participantes conozcan sus posturas y reflexiones sobre determinados temas a través de la creación de un "espectograma" de opiniones.
- **Duración:** 90 minutos
- **Formato:** Ejercicio
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - Una Internet Feminista[1]
- **Materiales requeridos:**
  - Una sala grande o un espacio exterior
  - ¡Tú misma!

El contenido de este ejercicio fue desarrollado por Mariel Garcia (SocialTIC) y Spyros Monastiriotis (Tactical Technology Collective).

[1] https://cyber-women.com/es/violencia-en-línea-contra-las-mujeres/una-internet-feminista/

Conducir la sesión

1. Arranca indicando dónde se ubican los dos extremos del Espectograma. Si están en un espacio interior, puede ser los dos extremos de la sala; si están afuera, puede ser la distancia entre dos árboles, paredes u otros puntos de referencia.
2. Cada uno de estos extremos representa una postura: "muy de acuerdo" y "muy en desacuerdo".
3. Explica el ejercicio: leerás en voz alta un enunciado (es importante plantearlas como afirmaciones y no como preguntas) y la volverás a repetir; las participantes se organizarán a lo largo del espectro "Muy de acuerdo-Muy en desacuerdo" según su postura con respecto a la afirmación. Evita confusiones y no uses frases que contengan doble negación.
4. Recuerda a las participantes que no tienen que escoger sólo un extremo u otro del espectro; pueden ubicarse en el punto medio si están indecisas o en cualquier punto según su nivel de acuerdo o desacuerdo con el enunciado.
5. En este espectrograma, la facilitadora leerá en voz alta varios enunciados relacionados con la seguridad digital y experiencias de mujeres en línea. Algunos ejemplos podrían ser:
    - No hay un motivo de peso para compartir la contraseña de tu cuenta de correo o de plataforma de red social.
    - A veces es necesario que nosotras, como mujeres, evitemos compartir ciertos puntos de vista online.
    - Tanto hombres como mujeres activistas enfrentan el mismo tipo de violencia y amenazas online.
    - Mi trabajo se hace imposible sin acceso seguro a espacios online.
6. Cada vez que las participantes se ubican en un punto del espectro al escuchar un enunciado, pide a 2 o 3 participantes que compartan su

postura. Estas aportaciones pueden detonar una discusión muy interesante.

7. Las participantes podrán cambiar de lugar después de haber escuchado los puntos de vista de las compañeras. Si sí lo hacen, pregúntales por qué.

Una Internet Feminista

- **Objetivos:** Brindar una oportunidad para generar conciencia sobre los retos que afrontan las mujeres en internet.
- **Duración:** 40 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - Her-Story (las historias de las mujeres) en las tecnologías[1]
  - Violencia simbólica[2]
- **Materiales requeridos:**
  - Rotafolio o papelógrafos
  - Marcadores de colores
  - Copias de Principios Feministas de Internet http://www.genderit.org/es/articles/principios-feministas-para-internet para cada participante

[1] https://cyber-women.com/es/repensar-nuestra-relación-con-las-tecnologías/herstory-en-las-tecnologias/

[2] https://cyber-women.com/es/violencia-en-línea-contra-las-mujeres/violencia-simbólica/

Conducir la sesión

Parte 1 – Generar conciencia

1. Arranca la sesión preguntándole a las participantes: ¿cuáles son algunos de los mensajes e ideas más comunes que han escuchado sobre mujeres y tecnologías? ¿Cuáles son las actitudes predominantes en relación a mujeres y tecnologías en sus países/contextos?
2. Las participantes crean una lluvia de ideas con algunos de los obstáculos que las mujeres afrontan cuando intentan acceder a las tecnologías y/o participan activamente en espacios en línea. Pueden hacerlo todas juntas o en grupos más pequeños. Como quieran. Anota las aportaciones del grupo(s) en el rotafolio.
3. Comparte algunas estadísticas generales y, si es posible, algunas más específicas en relación con las regiones y países de las chicas:
    - La penetración de uso de internet es más alto en el caso de hombres que mujeres en todas las regiones del mundo. La brecha de género es del 12%.
    - El 60% de los casos de violencia de género relacionado con las tecnologías digitales no es investigada por las autoridades.
    - Entre el 84 y 91% de los editores de Wikipedia son hombres.
    - Las mujeres ocupan el 27% de los puestos relacionados con gestión y dirección dentro de empresas de media y un 35% de la plantilla que trabaja en el sector de redacción.
    - Las mujeres que trabajan en tecnologías digitales ganan 28% menos que sus compañeros hombres, teniendo la misma formación, años de experiencia y edad.
4. Divide las participantes en grupos pequeños y pídeles reflexionar sobre las estadísticas compartidas anteriormente. ¿Cuáles son las implicaciones que tienen en las vidas de las mujeres y en la construcción de

un internet como espacio común que podamos habitar libremente?

Parte 2 - Principios feministas de internet

5. Introduce los "Principios feministas de internet de APC" como detonante de una reflexión sobre

   > (...) una internet feminista que se encamine hacia el empoderamiento de más mujeres y personas queer que puedan ejercer y disfrutar sus derechos, interactuar con placer y de manera lúdica; y desmantelar el patriarcado.

6. Entrega a cada grupo materiales impresos de los principios.
   - Acceso
   - Movimientos y participación pública
   - Economía
   - Expresión
   - Agencia
7. Pide a cada grupo discutir cómo cada principio se aplica en sus contextos y que hagan una lista de las maneras en que cada una pueda contribuir a transformar las realidades de las mujeres y las tecnologías.
8. Cada grupo presentará lo que haya reflexionado en conjunto y las conclusiones sacadas.

Referencias

- http://feministinternet.net
- https://es.wikipedia.org/wiki/Brecha_de_g%C3%A9nero_en_Wikipedia
- https://www.apc.org/es/pubs/principios-feministas-para-internet-version-2

Violencia simbólica

- **Objetivos:** Cómo identificar la violencia simbólica y cómo esbozar conexiones entre ella y la violencia de género en línea.
- **Duración:** 30-45 minutos
- **Formato:** Ejercicio
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - Espectrograma[1]
  - Una Internet Feminista[2]
- **Materiales requeridos:**
  - Rotafolio
  - Marcadores, lapiceros
  - Hojas de colores
  - Post-its
  - Cinta adhesiva

[1] https://cyber-women.com/es/violencia-en-línea-contra-las-mujeres/espectrograma/

[2] https://cyber-women.com/es/violencia-en-línea-contra-las-mujeres/una-internet-feminista/

Conducir la sesión

Parte 1 - ¿Qué es la violencia simbólica?

1. Arranca explicando qué significa el término “violencia simbólica”.

   La violencia simbólica se ejerce a través de imposiciones culturales de normas y comportamientos en relación al género. Se enseñan a las mujeres que “algo” nos puede pasar si andamos solas de noche, nos vestimos de cierta manera o si hacemos algo sin precaución. El miedo se convierte en un estado mental normalizado y aceptado.

   Esto implica que a nosotras, en tanto mujeres, nos responsabilizan por cualquier violencia que enfrentamos. Se engendra un estado de miedo y hasta terror que dibuja un “mapa mental de espacios prohibidas” para nosotras y suscita respuestas condicionadas como:

   - Sentir la necesidad de volver a casa de noche en un taxi o con un compañero varón.
   - Caminar más rápido o hasta corriendo cuando escuchamos pisadas detrás de nosotras.
   - Auto-censurarnos sin darnos cuenta en plataformas de medios sociales u otros tipos de plataformas.
   - Decidir no salir a la calle o no vestirnos de cierta manera por miedo a lo que nos podría pasar.

   Además, no sólo nos hacen responsables por la violencia que vivimos sino que no nos brindan estrategias y recursos para abordarla (aparte de las respuestas condicionadas de arriba), ni a disfrutar y ocupar los espacios, ni a ser libres en cómo nos movemos y hablamos en nuestros cuerpos y en nuestras sexualidades.

   La violencia simbólica crea espacios y situaciones prohibidas para las mujeres y nos niega nuestro derecho funda-

mental a la seguridad y a la libertad de movimiento. La impunidad de los agresores es un agravante a toda esta situación. A menudo, dichos agresores no son cuestionados sino patologizados como "locos" o inheremente incapaces de tomar control o responsabilidad sobre sus acciones.

Llegando a este momento de la sesión, quizás quieras discutir algunos imaginarios de la violencia que se ejerce contra las mujeres (violencia simbólica u otros tipos), normalizada por los medios de comunicación, especialmente en espacios online.

Parte 2 - Identificar la violencia simbólica contra nosotras mismas.

2. Entrega a cada participante post-its e indícales que anoten ejemplos de actividades que han dejado de hacer y comportamientos que han cambiado fruto de la violencia simbólica que han experimentado como mujeres ocupando espacios offline y online. Reúne de vuelta los post-its y lee algunos de los ejemplos en voz alta. Discútelas todas juntas, reflexionando sobre las posibles motivaciones detrás de estos cambios.
3. Explica que hay tres principales factores que construyen y habilitan el miedo y el terror en respuesta a la violencia simbólica:

   La apropiación del cuerpo femenino: el cuerpo femenino es visto como un objeto en un entorno masculino; ésto genera una ausencia de seguridad y confianza de la mujer hacia su cuerpo y sus capacidades.

   Culpa y vergüenza: consideradas como elementos permanentes e inamovibles que facilitan la percepción de que violencia de género perpetrada es merecida y, de cierta manera, aceptable.

   "Felicidad aprendida": estado psicológico que se genera con frecuencia cuando los eventos son percibidos como incontrolables, como si no se pudiera hacer nada para cambiar las consecuencias. El estado mental se adapta a través de la aceptación y normalización: sacrificamos nuestra agencia de tomar el control de vuelta.

4. Pregunta a las participantes qué estrategias creen que podrían transformar estos factores y abordar la violencia simbólica. Las pueden anotar en sus post-its. Compartimos algunas posibles estrategias:
    - Recuperar el control sobre la narrativa de nuestro cuerpo a través de resignificarla como territorio de placer y resistencia.
    - Reconocer y aceptar los daños que han sido ejercidos contra nuestro cuerpo (física y mentalmente), no como víctima sino como sobreviviente resiliente.
    - Construir y sostener redes de apoyo para nosotras, tanto online como offline. Nunca estamos solas en la lucha.

Referencias

- https://es.wikipedia.org/wiki/Indefensi%C3%B3n_aprendida
- http://www.autodefensafeminista.com/attachments/article/277/MANUAL%20Autodefensa%20Feminista.pdf

Denunciando el abuso en plataformas de medios sociales

- **Objetivos:** Compartir consejos para denunciar la violencia en línea que se ejerce en plataformas de redes sociales como facebook y twitter.
- **Duración:** 40 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - Campañas online más seguras[1]
  - Apps & Plataformas online: ¿Amigo/a o enemigo/a?[2]
  - ¡Empecemos a crear un diario de documentación![3]

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

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

[3]https://cyber-women.com/es/violencia-en-línea-contra-las-mujeres/empecemos-a-crear-

- **Materiales requeridos:**
  - Proyector y diapositivas
  - Post-its
  - Una computadora por cada dos participantes (si es posible)
- **Recomendaciones:** Esta sesión está especialmente dirigida a mujeres que han sido acosadas en línea o que están involucradas en campañas online.

Conducir la sesión

1. Arranca la sesión preguntando a las participantes:

   ¿Conocen colectivos de mujeres o activistas mujeres que hayan sido acosadas en línea? Si es así, ¿en qué plataformas?

   Pídeles que comparten ejemplos de tácticas que han visto que se utilizan o han utilizado ellas para afrontar el acoso en línea y que las escriban en post-its.

2. Comparte algunas recomendaciones de prácticas básicas para denunciar tipos de violencia comúnmente ejercidos contra las mujeres online, además de ONGs y colectivos que pueden brindar apoyo.

   La empresa Facebook recomienda reportar el comentario/post específico, dando el máximo contexto posible. Pueden leer sobre este proceso aquí: https://www.facebook.com/report

   Bloquear acosadore/as evita que recibamos solicitudes de amistad/suscripción o inicios de conversaciones, envío de mensajes o que dicha persona vea nuestras actualizaciones. Facebook no te notifica cuando te bloquean, pero te puedes dar cuenta en la medida que ya no puedes contactar con la otra persona.

   Toma capturas de pantalla antes de bloquear a quien/quienes te acosan para documentar pruebas del acoso porque, una vez que lo/as blo-

un-diario-de-documentación/

queas, se hace más difícil recopilar evidencias que puedas tener que presentar en una futura investigación sobre el incidente. Enseña a las participantes a sacar capturas si no saben hacerlo.

Twitter recomienda reportar el incidente y mantener el registro del número de caso para dar seguimiento. En Twitter puedes reportar tanto un tweet individual como un perfil entero.

Es recomendable evitar entrar en los links que te envían tu(s) acosadore/a(s), ya que pueden dirigirte a la instalación de malware en tu dispositivo.

3. Muestra cómo bloquear usuario/as y reportar perfiles y posts en Facebook y Twitter, además de otras plataformas de redes sociales que utilicen las participantes. Asegúrate de investigar estos procedimientos antes del taller para estar actualizada de cómo se hace. Estos procedimientos tienden a cambiar bastante (al igual que las configuraciones de privacidad).
4. Si quieres dedicar un tiempo a que las participen prueben por si mismas, divídelas en grupos pequeños e índicales que busquen páginas o perfiles que pueden ser blanco de acoso en línea. Pueden, por ejemplo, documentar posts o perfiles en Facebook que están propinando, de manera sistemática, acoso y reportarlas.

Referencias

- https://karisma.org.co/descargar/manualseguridadtw

¡Empecemos a crear un diario de documentación!

- **Objetivos:** Introducir prácticas que profundizan en la denuncia de abuso en línea, especialmente en el ámbito de la documentación de incidentes.
- **Duración:** 45 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - Denunciando el abuso en plataformas de medios sociales[1]
  - Hagamos doxxing al troll[2]
- **Materiales requeridos:**
  - Diapositivas (con los puntos claves descritos a continuación)
  - Computadora y proyector configurados

[1] https://cyber-women.com/es/violencia-en-línea-contra-las-mujeres/denunciando-el-abuso-en-las-plataformas-de-medios-sociales/

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

  - Copias impresas de la plantilla “Respaldo” (ver a continuación)
- **Recomendaciones:** Orientada a grupos que afrontan acoso en línea, han recibido amenazas online y offline, o que van a trabajar en proyectos o campañas que aumentan el riesgo a estar expuestas a acoso.

Conducir la sesión

Parte 1 - ¿Por qué la documentación es importante?

1. Explica

   ¿Qué es la documentación?

   La documentación, en este contexto, se refiere al abordaje sistemático y organizado de dar seguimiento a un incidente de abuso o acoso que ocurre en nuestro ámbito de trabajo. Básicamente, consiste en archivar pruebas.

   ¿Qué es un incidente?

   Un incidente es cualquier cosa que ocurre, tanto online como offline, que pueda constituir un abuso o acoso. Que un evento se clasifique como un incidente o no depende, sobre todo, del contexto y circunstancias en que ocurre y la gravedad de su impacto. Por ejemplo, si recibes un correo que parece un intento de phishing - y estás acostumbrada a recibir este tipo de cosas a menudo- quizás, de manera aislada, no sea suficientemente relevante como para considerarlo un incidente; sin embargo, si tu organización está a punto de lanzar una gran campaña y empiezas a recibir una cantidad atípica de correos, ahí sí es probable que podamos considerarlo un incidente y debe ser documentado.

   ¿Qué es un diario de documentación?

   Donde mantienes un registro de los incidentes que ocurren, de manera organizada para facilitar guardar información y evidencias importantes que después puedan servir de referencia.

¿Por qué la documentación es importante?

La documentación puede ser útil para volver a ella cuando estés intentando relacionar incidentes entre sí durante un periodo de tiempo determinado o entre personas de una misma organización. Puede revelar patrones de abuso u otros tipos de ataques en línea que de otra manera no te hubieras dado cuenta. Estos patrones pueden ayudarte a identificar un adversario/as o establecer conexiones entre diferentes tipos de incidentes y acciones que realizas tú o tu organización. Cuando reportas un abuso en una plataforma de red social, por ejemplo, pueden solicitar durante la investigación pruebas como capturas de pantalla y nombres de perfiles.

Parte 2 – ¿Cómo podemos documentar incidentes?

2. Entrega copias de la siguiente plantilla de "Cuaderno de documentación".
3. Aclara que estas plantillas sólo brindan un ejemplo de los tipos de información que puede ser importante recopilar cuando estás documentando un incidente. Puedes libremente agregar o quitar columnas y campos de la plantilla según vayas creando formatos más específicos que se ajusten a tu contexto de trabajo.

   Aquí incluímos dos plantillas: una para documentar incidentes en línea; otro para incidentes físicos/offline (en la siguiente página):

Plantilla de diario de documentación (Online)

Fecha
Hora
Resumen del incidente
Plataforma
URL

Captura de pantalla (nombre del archivo o copiar/pegar)
Descripción de la captura de pantalla/contenido
Nivel de riesgo
Pasos de seguimiento
Anotaciones

Plantilla de diario de documentación (offline/físico)

Fecha
Hora
Ubicación
Resumen del incidente
Personas involucradas
Nivel de riesgo
Pasos de seguimiento
Anotaciones

4. La mayoría de los campos de las plantillas son fáciles de entender; sin embargo, repásalos de todas maneras, describiendo brevemente qué significa cada uno y qué pretende monitorear.
5. Asegúrate de subrayar el campo de "Nivel de riesgo" ya que este parámetro es muy subjetivo y no tan claro como los demás. Como cada participante u organización define nivel de riesgo es extremadamente específico a su contexto. Puede ser útil parar en este punto y preguntarles a las participantes ejemplos de incidentes que definirían como bajo, medio y alto riesgo. Destaca que deberían considerar el impacto potencial de un incidente (a un nivel personal u organizacional o ambos) cuando estén definiendo un riesgo en este contexto.

   Opcional: ya sea antes o justo después de la sesión, repasa el ejercicio de "Modelo de riesgos con perspectiva de género". Durante el ejercicio,

el grupo tendrá una oportunidad de enfocarse en definir niveles de riesgo para su propio contexto. Pueden aplicar estas definiciones de riesgo en su cuaderno de documentación.

6. En último lugar, otro campo a destacar es "Pasos de seguimiento". Básicamente, un paso de seguimiento es lo siguiente que se va a abordar ante el incidente actual (por ejemplo, reportarlo en Facebook) o una medida que se va a implementar para prevenir que el incidente se repita o reducir su impacto.

   Opcional: ya sea antes o justo después de la sesión, repasa la sesión "Planes y protocolos de seguridad en organizaciones". Durante el ejercicio, el grupo tendrá una oportunidad de enfocarse en definir planes y protocolos de seguridad en respuesta a cierto tipo de riesgo conocido o potencial.

Parte 3 – Empezar nuestro cuaderno de documentación

7. Las participantes tienen 10-15 minutos para rellenar sus plantillas de documentación individualmente. Pueden rellenar la plantilla con detalles de incidentes actuales o usar ejemplos hipotéticos.

8. Una vez que hayan terminado la versión borrador de su cuaderno, las participantes se juntan en parejas y comparten los incidentes que documentaron. Tiene sentido que personas de la misma organización se junten en este paso para intercambiar impresiones sobre sucesos vividos por la organización. Cada persona formula preguntas a su pareja sobre el nivel de detalle y rigor de sus reportes. En algunos casos, ésto puede ayudar a la participante a recordar detalles específicos que quizás haya olvidado. Quizás algunas no se sientan cómodas compartiendo su cuaderno con las demás. En estos casos, déjales la opción de trabajar individualmente.

Parte 4 - Prácticas y consejos para mantener un cuaderno de documentación

9. Recuerda a las participantes que, para sostener la práctica de documentar en nuestro cuaderno, necesitaremos encontrar maneras para "socializar" o "integrar" su actualización en las rutinas cotidianas que llevamos a cabo. En el contexto de una organización, piensa si habrá una persona encargada de recopilar la información; quizás sea más fácil o más consensuado rotar esta tarea entre las personas del grupo o entre diferentes comisiones. Es recomendable que también comentes aquí que puede ser buena idea, si alguien adentro de la organización es el blanco del incidente, que otra persona sea quien lo documente.
10. Anima a las participantes a probar diferentes flujos de trabajo para encontrar maneras más eficientes de actualizar el cuaderno. Puede ser que encuentren formas de automatizar ciertas partes del proceso o puede ser que omitan ciertos campos de las plantillas que sean irrelevantes para su contexto.
11. Cierra la sesión preguntando a las participantes, ahora que han tenido tiempo para reflexionar sobre la importancia de documentar los incidentes que suceden en sus propios contextos, si sacan conclusiones clave de esta discusión o ideas para alimentar sus cuadernos.

Hagamos doxxing al troll

- **Objetivos:** Introducir herramientas y actividades centradas en recopilar información sobre acosadore/as. esta información puede ayudar a la hora de tomar decisiones en torno a la privacidad y seguridad en línea.
- **Duración:** 180 minutos
- **Formato:** Ejercicio
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Conceptos básicos de seguridad digital y/o capacitación previa.
  - Navegación más segura[1]
  - ¿Qué dicen tus metadatos sobre ti?[2]
- **Sesiones y ejercicios relacionados:**
  - Navegación más segura[3]
  - ¿Qué dicen tus metadatos sobre ti?[4]

[1]https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/navegación-más-segura/

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

[3]https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/navegación-más-segura/

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

  - ¡Empecemos a crear un diario de documentación![5]
- **Materiales requeridos:**
  - Copias impresas de la plantilla de "Diario de documentación" (disponible online)
  - Diapositivas (con los puntos clave descritos a continuación)
  - Computadora y proyector configurados
- **Recomendaciones:** Este ejercicio está recomendado para grupos de defensoras que están viviendo, o vivieron recientemente acoso en línea. aunque no es estrictamente necesario, este ejercicio funciona mejor si el grupo ya participó en la sesión de "¡empecemos a crear un diario de documentación!". recomendamos que cada participante tenga su propio dispositivo móvil o computadora. quizás quieras dividir la sesión en dos partes puesto que es larga. también puedes hacerla en una sesión, pero con un descanso largo en medio.

Este ejercicio es una adaptación de la actividad desarrollada por Indira Cornelio (SocialTIC) y Phi Requiem (#SeguridadDigital), en colaboración y con el apoyo de "Dominemos las Tecnologías" de APC.

Conducir la sesión

Parte 1 – ¿Qué es el Doxxing?

1. 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.
2. Subraya lo siguiente:

sobre-ti/

[5] https://cyber-women.com/es/violencia-en-línea-contra-las-mujeres/empecemos-a-crear-un-diario-de-documentación/

El objetivo de este ejercicio no es recomendar el doxxing como una buena práctica (o recomendar métodos ilegales o cuestionables para hacerlo) ya que implica la revelación pública de información personal. Enfatiza que exponer la identidad o información sobre una persona no es necesario. Más bien, lo que se quiere lograr en la sesión es que las participantes aprendan a obtener este tipo de información online para ayudarlas a tomar decisiones fundamentales sobre cómo abordar el abuso y acoso.

3. Finalmente, repasa con ellas prácticas de navegación segura. Parte de este ejercicio implica visitar perfiles y sitios online de los acosadores.

Parte 2 – Identificar lo/as acosadore/as

4. Establezcan las expectativas de cada una para el ejercicio: ¿Qué quieres averiguar de tu acosador/a? Comenta varios posibles motivos de antemano:

- ¿Quieres descubrir su identidad real?
- ¿Quieres entender sus motivos?
- ¿O si están acosando a otras defensoras también?
- ¿Si están actuando una o varias personas?

5. Puede ser que algunas participantes hayan escuchado maneras de obtener este tipo de información sobre sus acosadore/as, pero aclara que las herramientas y tácticas que van a utilizar en la sesión tiene ciertas limitaciones. Si el grupo ya ha participado en la sesión "¡Empecemos a crear un diario de documentación!", recuérdales la importancia de recopilar pruebas como paso crítico para detectar patrones de acoso y poder denunciarlo. Si aún no han participado en esta sesión, comenta que, más adelante en la sesión, revisarán un método para dar seguimiento a incidentes de acoso.

Parte 3 - Diferentes perfiles, diferentes motivos

6. Comparte algunos casos de mujeres activistas o periodistas y sus experiencias con el acoso en línea. Intenta encontrar casos que sean relevantes a los contextos de las participantes y que muestren perfiles diversos de acosadore/as y motivos.
7. Si alguna participante se siente cómoda compartiendo, puede comentar su propia experiencia al respecto. ¿Cuándo empezó? ¿Quién cree que es? ¿Es una persona conocida para ella? ¿Se les ocurre alguna motivación concreta que pueda tener?
8. Reflexiona sobre los posibles fines y razones que pueda tener la persona acosadora. ¿El acoso se debe a que eres mujer? ¿Porque defiendes derechos de las mujeres/humanos? ¿Has observado este tipo de acoso en tus compañeros varones? Si es así, ¿ocurre de la misma manera o tiene rasgos distintivos?

Parte 4 - Documentar incidentes & amenazas

9. Si el grupo ya participó en la sesión "¡Empecemos a crear un diario de documentación!", repasa las conclusiones clave y explica cómo la práctica de documentación es un componente importante en obtener información sobre personas acosadoras y tomar decisiones sobre la manera de proceder. Puedes saltar directamente a la Parte 5 - Preparativos
10. Si las participantes aún no han realizado esta sesión, arranca explicando los siguientes puntos que subrayan la relevancia de la documentación a la hora de abordar el acoso en línea:

    ¿Qué es la documentación?

    La documentación, en este contexto, se refiere al abordaje sistemático y organizado de dar seguimiento a un incidente de abuso o acoso que ocurre en nuestro ámbito de trabajo. Básicamente, consiste en archivar pruebas.

Qué es un incidente?

Un incidente es cualquier cosa que ocurre, tanto online como offline, que pueda constituir un abuso o acoso. Que un evento se clasifique como un incidente o no depende, sobre todo, del contexto y circunstancias en que ocurre y la gravedad de su impacto. Por ejemplo, si recibes un correo que parece un intento de phishing - y estás acostumbrada a recibir este tipo de cosas a menudo- quizás, de manera aislada, no sea suficientemente relevante como para considerarlo un incidente; sin embargo, si tu organización está a punto de lanzar una gran campaña y empiezas a recibir una cantidad atípica de correos, ahí sí es probable que podamos considerarlo un incidente y debe ser documentado.

¿Qué es un diario de documentación?

Donde mantienes un registro de los incidentes que ocurren, de manera organizada para facilitar guardar información y evidencias importantes que después puedan servir de referencia. ¿Por qué la documentación es importante? La documentación puede ser útil para volver a ella para relacionar incidentes entre sí durante un periodo de tiempo determinado o entre personas de una misma organización. Puede revelar patrones de abuso u otros tipos de ataques en línea que de otra manera no te hubieras dado cuenta. Estos patrones pueden ayudarte a identificar a adversario/as o establecer conexiones entre diferentes tipos de incidentes y acciones que realizas tú o tu organización. Cuando reportas un abuso en una plataforma de red social, por ejemplo, pueden solicitar durante la investigación pruebas como capturas de pantalla y nombres de perfiles.

11. Ahora puede introducir el cuaderno de documentación a las participantes. Para este ejercicio, puedes utilizar solamente la versión online. Imprime versiones de la plantilla antes del taller y entrégalos al grupo. Véase plantilla a continuación:

Plantilla de diario de documentación (Online)

Fecha
Hora
Resumen del incidente
Plataforma
URL
Captura de pantalla (nombre del archivo o copiar/pegar)
Descripción de la captura de pantalla/contenido
Nivel de riesgo
Pasos de seguimiento
Anotaciones

12. Aclara que estas plantillas sólo brindan un ejemplo de los tipos de información que pueden ser importantes recopilar cuando estás documentando un incidente. Pueden libremente agregar o quitar columnas y campos de la plantilla según vayan creando formatos más específicos que se ajusten a su contexto de trabajo.
13. La mayoría de los campos de las plantillas son fáciles de entender; sin embargo, repásalos de todas maneras, describiendo brevemente qué significa cada uno y qué pretende monitorear.
14. Asegúrate de subrayar el campo de "Nivel de riesgo" ya que este parámetro es muy subjetivo y no tan claro como los demás. Como cada participante u organización define nivel de riesgo es extremadamente específico a su contexto. Puede ser útil parar en este punto y preguntarles a las participantes ejemplos de incidentes que definirían como bajo, medio y alto riesgo. Destaca que deberían considerar el impacto potencial de un incidente (a un nivel personal u organizacional o ambos) cuando estén definiendo un riesgo en este contexto.
15. Las participantes tienen 10-15 minutos para rellenar sus plantillas de documentación individualmente. Pueden rellenar la plantilla con detalles de incidentes actuales o usar ejemplos hipotéticos.

Parte 5 – Preparativos

16. Antes de seguir, es importante recalcar que no entren en los enlaces que pueden llegar a recibir o encontrar cuando están haciendo doxxing de su acosador/a. Estos enlaces pueden ser intentos de phishing (explica este concepto si no la conocen) que buscan engañarte en instalar software malicioso en tus dispositivos. Destaca la gran importancia de evitar entregar información adicional a tu(s) acosadore/a(s); en el mismo sentido, para las participantes que no están enfrentando acoso en la actualidad, es deseable que eviten llamar la atención innecesariamente que pueda desencadenar en acoso.
17. Repasa con las participantes los siguientes pasos para recopilar información sobre sus acosadores/as de manera segura.
    - Recomendamos que reúnan cualquier información que ya pueden tener sobre ello/as y documentar los incidentes en sus cuadernos de documentación.
    - Escojan el navegador web que van a utilizar para su investigación y procuren salir de sus sesiones de cuentas y borrar su historial y cookies. Lo mejor sería utilizar el navegador Tor para esta actividad, si ya han repasado esta herramienta.
    - Quizás quieran considerar crear nuevas identidades o perfiles online para realizar este ejercicio (una cuenta falsa en Facebook, Twitter o Gmail). Recuérdales que tengan cuidado de no usar información que pueda rastrearlas a sus "identidades reales".
    - Haz énfasis en la importancia de documentar, de tomar anotaciones durante el proceso.
    - Pueden crear una carpeta expresamente para esto en sus computadoras con el fin de recopilar y almacenar cualquier información y pruebas de este ejercicio, como por ejemplo imágenes de avatares, capturas de pantalla, nombres de usuario, cuentas de correo y plataformas de redes sociales, comentarios en foros, comentarios sobre ubicaciones o contactos conocidos.

Parte 7 – Herramientas útiles

18. Ahora puedes empezar a compartir ejemplos de herramientas que puedan ser útiles para su investigación de doxeo. Cuando sea posible, ofrece una copia de tu presentación con toda esta información o un material entregable con una lista de herramientas y enlaces para que puedan volver a ella después para profundizar.
19. Explica cada herramienta y genera el tiempo para que puedan buscarlas en internet y probarlas. Aparte de las que aparecen en la lista a continuación, puedes agregar otras que conoces que consideres que puedan ser útiles o relevantes:
    - Considera cifrar tus discos.
    - Deja Google y usa StartPage[6] o DuckDuckGo[7].
    - Recomienda usar Tails[8] o cuando no sea posible, usar el navegador Tor[9].
    - Búsqueda avanzada en Twitter[10].
    - Checa http://whois.net para buscar información vinculada a un sitio web como quién es propietario/a del dominio.
    - Búsqueda inversa de imágenes en Google[11] para rastrear imágenes y fotos que hayas podido recibir.
    - Herramientas de metadatos en caso de que hayas recibido imágenes o fotos:
      - MetaShield[12]
      - MetaPicz[13]

[6] https://startpage.com
[7] https://duckduckgo.com
[8] https://tails.boum.org
[9] https://www.torproject.org
[10] https://twitter.com/search-advanced
[11] https://images.google.com/
[12] https://www.elevenpaths.com/technology/metashield/index.html
[13] http://metapicz.com

- Social Mention ("Mención social")[14];
- Follower Wonk[15];
- NameCheck ("Verificar nombres")[16];

20. Explica que hay maneras de construir sistemas simples de monitoreo online que funcionan especialmente bien cuando queremos seguirle la pista a ciertos nombres de perfil, usuario o hashtag.

- IFTTT[17] – explica cómo permite a las usuarias conectar Twitter con Google Drive para monitorear tweets y menciones vinculadas a cierta cuenta de usuario/a o hashtag.
- Google Alerts[18]
- Tweetdeck[19]

21. Dependiendo del tiempo que tengan, las participantes pueden realizar su investigación durante el taller o hacerlo para la siguiente sesión. Sea de una manera u otra, recuérdales que será útil - una vez que hayan recopilado información - dar un paso atrás y mirar todos los datos que han reunido:
    - ¿Observan patrones emergentes?
    - ¿Qué revela la información sobre su acosador/a?
    - Quizás puedan hasta predecir futuros blancos potenciales o tipos de ataques.

Referencias

- https://www.apc.org/es/pubs/issue/como-evitar-convertirse-en-una-victima-del-ciberac

[14] http://socialmention.com
[15] https://moz.com/followerwonk
[16] https://namechk.com
[17] https://ifttt.com
[18] https://www.google.com/alerts
[19] https://tweetdeck.twitter.com

- https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/es#Lidiar_con_Trols
- https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/es#Bots_contra_trols