Image not found or type unknown

¡Respalda! ¡Bloquea! ¡Elimina! También conocido como alguien tomó mi celular: cruzar fronteras, detenciones, incautación y robo [actividad táctica]



En esta actividad, planearemos y realizaremos los preparativos para situaciones donde nuestros celulares pueden estar bajo riesgo físico. Algunas situaciones pueden incluir:

- Temas de seguridad a la hora de participar en protestas y marchas
- Temas de seguridad a la hora de cruzar fronteras
- Temas de seguridad cuando hay riesgo de detención y incautación

- Temas de seguridad cuando hay riesgo de robo y acoso

Esta actividad consiste en 4 etapas con la opción de una parte más práctica dedicada a instalar y configurar dispositivos.

- Prácticas actuales de cuidado
- Planear y configurar nuestros dispositivos
- Presentación - Opcional

Si quieren, terminen esta actividad con una parte más práctica para aplicar estrategias y tácticas.

Objetivos de aprendizaje

- familiarizarse con la seguridad celular partiendo de la idea de que los celulares son tanto herramientas para nuestra vida personal y privada como en la esfera pública y en nuestras redes activistas;
- obtener una noción básica de cómo funciona la comunicación celular y de los riesgos implicados;
- adquirir y practicar estrategias y tácticas de seguridad celular para gestionar los impactos de la comunicación celular en nuestras vidas y las de nuestras compañeras y redes activistas;

¿Para quién es esta actividad?

Para participantes con diferentes niveles de experiencia utilizando celulares para poner en práctica la seguridad táctica con especial enfoque en los cuidados y dispositivos.

Tiempo requerido

Aproximadamente **80 minutos**.

Materiales requeridos

- Papeles grandes/rotafolios/pizarrón + marcadores

Mecánica

Este ejercicio está diseñado para apoyar a activistas que tienen la intención de interactuar en situaciones arriesgadas con sus celulares. Como resultado de esta actividad, tendrán un mapa de herramientas y tácticas que pueden utilizar.

Prácticas actuales de cuidado digital - 20 minutos

> **Consideraciones de cuidados:** *en esta actividad táctica planeamos y nos preparamos para usar nuestros celulares en situaciones donde, tanto nosotras como nuestros dispositivos, se exponen*

Empieza recalcando que prepararse para una situación arriesgada implica considerar primero cómo nos cuidamos antes, durante y después de la acción.

A través de una discusión grupal, comparte qué diferentes maneras tienen de cuidarse en situaciones de mucho riesgo. A nivel individual, responde a las siguientes preguntas:

- Entre las situaciones en las que participas, ¿en qué casos necesitas considerar tu seguridad física y la de tu dispositivo?
- ¿Qué estás haciendo ya para cuidarte - antes, durante y después - en estas experiencias?

Divide el papel en 3 secciones: antes, durante y después. Se verá algo así como:

Ejemplo

ANTES	DURANTE	DESPUÉS

Una vez contestada las preguntas, compartan en el grupo sus respuestas, tanto prácticas que realizan por su cuenta como las que hacen con otras personas. Anota en un pizarrón o papel grande palabras clave que salen de las aportaciones. Deja visible esta constelación de palabras.

Las participantes seguirán utilizando este método sencillo para organizar la siguiente parte del taller.

Planear y configurar nuestros dispositivos - 45 minutos

Si estás trabajando con participantes que están organizando un evento, realiza el ejercicio basado en eso. En caso contrario, estos escenarios descritos a continuación pueden servir. Son ejemplos y te invitamos a apropiarte de ellos, modificarlos e inventar tus propias situaciones.

Escenario 1: Temas de seguridad a la hora de participar en protestas y marchas

Vas a participar en una marcha/protesta masiva. Necesitas poder mantener segura la información almacenada en tu celular y evitar que te rastreen en la protesta/marcha, pero también necesitas utilizar tu celular para contactar con aliadas en caso de emergencias. También estás pensando en utilizar tu celular para documentar la marcha/protesta y cualquier posible violación a los derechos humanos que pueda pasar.

Escenario 2: Temas de seguridad a la hora de cruzar fronteras (inseguras)

Estás viajando y vas a cruzar la frontera hacia una ubicación insegura. Quieres utilizar tu celular para mantenerte en contacto con aliadas sin que otras personas ajenas te rastreen. Pregunta a las demás qué estrategias tienen cuando saben que quizás alguien tenga acceso a su dispositivo. Algunos ejemplos de situaciones pueden incluir cruzar la frontera, subirse a un avión, ir a una protesta/marcha.

Escenario 3: Temas de seguridad cuando hay riesgo de detención y incautación

Te has enterado, a través de un contacto de confianza, que te están fichando por parte del Estado y pretenden detenerte y confiscar tus dispostivos debido a tu activismo.

Escenario 4: Temas de seguridad cuando hay riesgo de robo y acoso

Te preocupa que alguien pueda robarte el celular y utilizar el contenido almacenado para acosarte.

Pide a las participantes documentar sus discusiones sobre papeles que tengan 3 secciones: antes, durante y después. Se verá algo así como:

EJEMPLO

ANTES	DURANTE	DESPUÉS

En grupos pequeños, deja tiempo para discutir las siguientes preguntas:

¿Qué riesgos e impactos viven las personas (en este escenario o en el evento que está planeando el grupo)? ¿Quiénes viven estos impactos? Toma en cuento a ti, a las personas que están en tu celular de alguna manera (es decir, información sobre ella), tus actividades (temas y eventos en los que estás trabajando), etc.

Puedes basarte en las siguientes preguntas como orientación para reducir los impactos desde una perspectiva táctica.

Antes: piensa en qué harás para preparar tu celular para este escenario.

- ¿Qué archivos vas a eliminar? ¿Por qué?
- ¿Qué aplicativos vas a instalar? ¿Por qué?
- ¿Vas a avisar a gente sobre tus planes?
- ¿Vas a acordar, entre un grupito de personas, un protocolo de seguimiento para saber cómo está cada quien antes y después de la actividad si es posible?
- ¿Qué formas de comunicación segura vas a utilizar con las demás personas?
- ¿Qué otros tipos de estrategias vas a implementar con tus aliadas para mantenerse seguras durante la actividad?

Durante: piensa cómo vas a utilizar tu celular en este escenario.

- Fuente de electricidad: ¿es un tema que hay que considerar?
- ¿Cómo vas a asegurar que las personas puedan cargar sus celulares?
- Servicio: ¿es un tema que hay que considerar?
- ¿Qué vas a hacer si alguien no puede usar/acceder a su servicio telefónico, aplicativos o datos?
- ¿Tienen algún plan/protocolo/procedimiento fuera de internet?
- ¿Con quién(es) quieres comunicarte en esta situación? ¿Cómo lo harás?
- ¿Estás documentando la protesta/marcha? En caso afirmativo, ¿estás utilizando algún aplicativo en particular?
- ¿Quién podrá contactarte a través del celular?
- ¿Y con quién(es) vas a contactar?
- Si vas a utilizar otra tarjeta SIM, ¿cómo vas a escoger un proveedor telefónico?
- ¿Sabes si algunos son más seguros que otros?
- ¿Quién(es) podrán contactar contigo?
- ¿Con quién(es) te vas a contactar?

Después: piensa qué vas a hacer después de este escenario.

- Archivos multimedia: si aplica, ¿qué vas a hacer con las grabaciones, fotos, audios y otros archivos multimedia que recopilaste?
- Metadatos y registros que tu celular genera: ¿qué medidas necesitas tomar sobre los datos que tu celular genera en este contexto (tomando en cuenta los metadatos, los historiales y las ubicaciones dispositivo)?
- En caso de incautación: ¿cómo sabes si tu celular no tiene spy-ware?
- En caso de robo o incautación: ¿qué vas a hacer para restaurar la integridad y seguridad de tu celular?

Deja entre 30 y 45 minutos para que los grupos puedan pensar en planes, estrategias y tácticas. Después comparte en plenaria las diferentes respuestas. Utiliza estas respuestas para planear una sesión práctica de seguridad celular.

Presentación (opcional) - 15 minutos

Anotaciones para facilitar la sesión: según tu forma de trabajar y cómo son tus participantes, quizás quieras profundizar y complementar con alguna presentación. A continuación incluimos anotaciones que creemos que pueden ser útiles para planear la sesión.

Antes

- Recalca que los escenarios planteados son situaciones donde hay una preocupación sobre nosotras mismas y nuestras pertenencias. Realiza planes para verificar con alguien de confianza que todo está bien antes y después de la situación. La frecuencia con la que verificas con esta(s) persona(s) puede variar según el nivel de riesgo de la situación.
- Para situaciones de alto riesgo: recomendamos verificar hasta cada 10 minutos. Por ejemplo, si vas a ir a una protesta/marcha de mucho riesgo o vas a cruzar una frontera peligrosa.
- Para situaciones de riesgo bajo: por ejemplo, estás trabajando con un grupo de trabajadoras sexuales y vas a estar moviéndote a diferentes lugares y participando en diferentes reuniones. Planea verificar con alguien de confianza cada vez que te desplazas al siguiente lugar de reunión y al llegar al destino. Avisa también al empezar y terminar el día con mensajes sencillos como "ya llegué", "voy empezando el día".
- Limpieza: ¿qué tienes en tu dispositivo que quieres mantener privado?
- Cierra sesión: sal de tus sesiones cuando no las estás utilizando. No las mantengas abiertas si no necesitas utilizar el servicio. Si alguien toma tu celular y están abiertas tus sesiones, podrán acceder a tus cuentas, ver qué haces y hacerse pasar por ti.
- Bloquea y cifra: puedes cifrar tu celular, tarjeta SD y tarjeta SIM, cada uno con su propia clave PIN de tal manera que, aunque acedan a tu dispositivo, no pueden acceder a la información. También, en caso de acceder a uno de estos lugares, no pueden acceder a los demás porque tienen claves distintas. *Si estás en una situación donde te están amenazando si no das acceso a tu información, quizás no puedas mantener tus claves y contraseñas privadas. Toma esto en cuenta en tus protocolos de seguridad y habla con otras personas sobre ello.*
- Copia de dispositivos: muchas agencias de policía tienen acceso a equipos que hacen copias digitales de dispositivos como celulares, laptops y discos duros. Si tu dispositivo está cifrado, aunque hagan una copia, no podrán acceder a la información sin la clave. En caso contrario, podrán acceder a los contenidos a través de esta copia.

- Silenciar: deshabilita el sonido y los avisos visuales de tus notificaciones, ponlo en modo silencio.
- Eliminar archivos remotamente: en algunas situaciones, quizás quieras habilitar esta función para asegurar que tú u otros contactos de confianza puedan borrar remotamente el contenido de tu celular en caso de que alguien sin consentimiento consiga acceder a él o en caso de pérdida/extravío.
- Tarjetas SIM y dispositivos: nuestros celulares son dispositivos que crean y comparten mucha información, desde mensajes y llamadas hasta datos de aplicativos y metadatos como ubicación y fechas. Evalúa si quieres llevar tus dispositivos personales encima en situaciones arriesgadas. En caso afirmativo, tus oponentes/adversarios pueden asociarte a tu dispositivo y rastrearte. También puedes dejar tu dispositivo personal en casa o utilizar algún dispositivo "desechable"("burnout") que planeas utilizar sólo para esta acción o evento, partiendo ya del presupuesto que lo van a asociar a ti, pero que podrás desecharlo después. Toma en cuenta que vas a necesitar tanto un celular como una tarjeta SIM para seguir este método. Y ambos tienen un identificador. Si utilizas tu teléfono y otra tarjeta SIM y después vuelves a meter tu tarjeta SIM, vincularán estas identidades. *Esta estrategia implica una inversión de dinero y energía: evitar que no te rastreen a través del celular y tarjeta SIM implica planear mucho y poder desechar el dispositivo. Si no tienes las condiciones para ello, puedes utilizar un dispositivo alternativo cada vez que participas en una situación arriesgada, pero tomando en cuenta que conforme lo vayas utilizando más y más, será más fácil vincularte a este aparato.*
- Sacar tarjetas SIM: si te encuentras en una situación arriesgada sin haberlo planeado, puedes sacar partes de tu teléfono como tu tarjeta SIM o tarjeta de memoria (en caso de que sea posible). *Observación: en algunas situaciones, esto puede ser utilizado como pretexto por parte de agresores para incrementar el daño que causan.*

Durante

- Eliminar archivos remotamente
- PixelKnot para cifrar mensajes
- Firechat para protestas/marchas y cortes de red

Cuando tu celular ha estado fuera de tu control

- Formatea o sustituye por un dispositivo nuevo: recomendamos restaurar la versión de fábrica. Si puedes permitírtelo económicamente, reemplaza el dispositivo; no resetees tu dispositivo anterior sino déjalo con alguien que pueda analizarlo.
- Tus servicios: cambia las contraseñas de todas tus cuentas.
- Avisa a la gente: si tu celular ha estado fuera de tu control, avisa a tus contactos y las personas con las que has estado manteniendo comunicación e infórmalas sobre las posibles implicaciones.

Materiales complementarios

- EFF Autoprotección Digital Contra La Vigilancia - Cómo cifrar su iPhone - https://ssd.eff.org/es/module/c%C3%B3mo-cifrar-su-iphone
- EFF Autoprotección Digital Contra La Vigilancia - Cómo utilizar Signal en iOS - https://ssd.eff.org/es/module/c%C3%B3mo-utilizar-signal-en-ios
- EFF Autoprotección Digital Contra La Vigilancia - Cómo utilizar Signal en Android - https://ssd.eff.org/es/module/c%C3%B3mo-utilizar-signal-en-android
- EFF Autoprotección Digital Contra La Vigilancia - Cómo utilizar Whatsapp en iOS - https://ssd.eff.org/es/module/c%C3%B3mo-utilizar-whatsapp-en-ios
- EFF Autoprotección Digital Contra La Vigilancia - Cómo utilizar Whatsapp en Android - https://ssd.eff.org/es/module/c%C3%B3mo-utilizar-whatsapp-en-android

image-1605451259399.png
Image not found or type unknown

Revision #4
Created 26 April 2023 00:29:00 by Kira
Updated 28 June 2023 18:53:21 by Kira