¿Qué es un celular? ¿Cómo funciona la comunicación telefónica? [actividad de profundización]

El objetivo de esta actividad es profundizar en cómo funciona la comunicación telefónica para poder evaluar y planear los potenciales riesgos. Se recomienda, en cualquier taller sobre celulares, verificar si las participantes cuentan con esta información de base y, en caso contrario, incluir este ejercicio. Se trata de un punto de partida fundamental para poder evaluar riesgos técnicos relacionados con los celulares.

Esta actividad tiene 2 etapas:

- Sesión práctica: desmontar celulares
- Introducción: los datos generados en la comunicación telefónica y consideraciones sobre riesgos.

Objetivos de aprendizaje

- obtener una noción de los conceptos básicos de cómo funciona la comunicación telefónica y de los posibles impactos implicados.

¿Para quién es esta actividad?

Esta actividad es para cualquier persona que participa en un taller sobre celulares.

Tiempo requerido

Aproximadamente **45 minutos.**

Materiales requeridos

- algunos celulares para desmontar e investigar
- un pizarrón, diapositivas o material impreso con apuntes de los contenido

Mecánica

Menciona o discute más en profundidad (según el tiempo disponible) que en esta sesión estarán abordando tecnologías móviles - considerando que son dispositivos fácilmente portables (en nuestras manos o en nuestros bolsillos) y nos permiten comunicarnos (a través de llamadas de voz, sms, navegación web). Esta sesión también aplica a tablets.

Adentro de nuestros celulares - 5 minutos

¡Ahora toca desmontar nuestros teléfonos! Los celulares son como computadoras pequeñas. Ubiquemos las diferentes partes de nuestros dispositivos:

- Las partes que escuchan y proyectan sonido: micrófonos, altavoces/bocinas
- Las partes que ven y muestran visuales: cámaras, pantallas
- Las partes que envían y reciben información de otras fuentes: GPS, antena, WiFi
- Partes de la computadora, hardware: batería, circuitos
- Memoria: tarjeta SD, otras memorias integradas en las ranuras
- SIM del teléfono

Identidad de la tarjeta SIM + identidad del teléfono - 5 minutos

Tu teléfono se compone de todas estas piezas y tiene varios rasgos identificativos; aparte de la marca, modelo y sistema operativo, también tiene dos nombres: un identificador de dispositivo y un identificador de tarjeta SIM. Es importante conocerlos porque nuestros celulares comunican esta información hacia fuera a menudo, especialmente el identificador SIM (IMSI) y nos pueden identificar a través de estas características.

- **IMEI**: nombre del dispositivo.

Identidad internacional de equipo móvil (IMEI): https://es.wikipedia.org/wiki/IMEI

- **IMSI**: nombre de tu tarjeta SIM

Identidad Internacional de Suscripción al Servicio Móvil (IMSI): https://es.wikipedia.org/wiki/IMSI

Nuestros celulares comunican - 35 minutos

Utilizamos nuestros teléfonos para comunicarnos con personas: SMS, mensajes, plataformas de redes sociales, aplicativos, llamadas. Nuestros celulares también comparten información sobre nuestros teléfonos y nosotras mismas - no sólo nuestros mensajes, pero también metadatos como nuestra ubicación, etc. Estos metadatos pueden vincularse a más información sobre nosotras como nuestras redes sociales, nuestras redes activistas/organizativas y nuestros lugares de trabajo.

Es relevante tomar esto en cuenta, sobre todo para entender que nuestros celulares pueden ser dispositivos de rastreo en tiempo real y almacenar un registro de nuestras actividades.

1. A nuestros celulares les gusta hablar

Nuestros teléfonos intentan hablar con diferentes tipos de redes a su alrededor para anunciar que está cerca, para ver si se puede conectar a alguna red y para averiguar si alguien se quiere conectar al dispositivo.

Empresas de telefonía

Hay torres y antenas con las que se comunica tu celular. Cada antena tiene un cierto alcance. Tu celular se comunica con cualquier torre que queda cerca y comparte, **como mínimo, tu IMSI** (para informar qué empresa de teléfono estás utilizando) y tu número (para que puedas recibir mensajes, llamadas y otros tipo de comunicación en tu dispositivo). Cada vez que estás cerca de

una torre es como si estuvieras colocando un marcador indicando dónde estás en cada momento y qué estás haciendo según el uso que das a tu celular.

GPS

Cuando está activado, tu celular se comunica con satélites GPS, también informando dónde estás en cada momento.

Wifi

Si está habilitado, en la medida que pases cerca de alguna red WiFi, tu dispositivo puede intentar conectarse a ella y dejar un rastro de que estuviste ahí (tanto en la red como en tu celular).

Bluetooth/NFC

Cuando está activado, otros dispositivos que usan Bluetooth y NFC pueden comunicarse con tu dispositivo, intentar conectarse y compartir archivos.

Discusión grupal: ¿qué funciones necesitas activar en cada momento? ¿Tener registros de dónde has estado implica un riesgo para ti?

2. A ti te gusta hablar

Utilizamos nuestros celulares para comunicarnos. Los diferentes tipos de comunicación aparecen de manera diferente:

SMS

Mensajes de texto y metadatos - aparecen en texto plano a la hora de enviarse y almacenarse en tu dispositivo y en la infraestructura de las empresas de telefonía. Una analogía útil es pensar que los SMS son como cartas postales. Si alguien la intercepta, puede ver todo su contenido y sus metadatos (por ej, quien lo envía y lo recibe, fecha).

MMS

Contenidos multimedia y metadatos - si alguien intenta interceptar tu comunicación, podrá verla o no según los mensajes estén cifrados o no. Al enviar estos mensajes MMS, tu proveedor de telefonía celular y los proveedores de las personas con las que te estás comunicando guardan un registro de los contenidos y metadatos (quién envía/recibe, fecha).

Llamadas

Contenido de llamadas y metadatos - supuestamente las llamadas deberían estar cifradas, pero tu proveedor de telefonía y los proveedores de las personas con las que te estás comunicando almacenan metadatos sobre la llamada (por ej, quien envía/recibe, fecha). Si alguien accede a estas empresas de telefonía, pueden llegar a esuchar y grabar llamadas.

Para más información sobre Apps y Mensajería, véase:

- Conversación, intro + sesion práctica: Escoger apps celulares

Comentario sobre vigilancia estatal: varía según el país. En algunos lugares, los gobiernos tienen acceso a cualquer dato gestionado por las empresas de telefonía -- en estos casos, considera que todos los contenidos y metadatos que se envían y guardan en servicios sin cifrar pueden ser accedidos por gobiernos, tanto en tiempo real como a posteriori durante una investigación.

Tu mejor mecanismo de defensa contra la vigilancia es usar cifrado de extremo a extremo.

3. Un teléfono es una computadora pequeña

Bug de software - un teléfono es una computadora y puede estar infectada de malware igual que una compu de escritorio o laptop. Tanto personas como gobiernos utilizan este tipo de software para meterse en los dispositivos de otras personas. El malware suele utilizar partes del teléfono para funcionar como un "bug" o dispositivo de rastreo para escuchar a través del micrófono o datos de ubicación.

4. La nube es un archivero

Nuestros celulares también acceden a datos que están en la "nube", es decir, en "internet", o más bien, en un dispositivo que está conectado a internet. Tus apps pueden estar accediendo a datos que están en la nube y no en tu dispositivo.

Consideraciones: ¿los datos enviados entre mi celular y mis servicios están cifrados? ¿están cifrados cuando están almacenados? ¿Conozco casos en los que personas o grupos adversarios pueden tener acceso a esta información? ¿Cuándo? ¿Cómo?

Nota de facilitación: mientras hablas, las participantes pueden hacer preguntas sobre partes de sus celulares o los riesgos asociados a los métodos de comunicación que compartes. Toma tiempo en responder a las pregutnas. Si puedes, toma nota en un pizarrón o un papel grande sobre los temas que van saliendo, incluyendo los que no se van a poder cubrir en el taller, pero que puedas dar seguimiento después para mandar más información.

Materiales complementarios

- Materiales sobre celulares en el portal ciberfeminista Ciberseguras: https://ciberseguras.org/?s=celular
- Cibermujeres Módulo Celulares más seguros https://cyber-women.com/es/celulares-m%C3%A1s-seguros/

- 7 maneras de encontrar tu número IMEI o MEID en tu celular (inglés): http://www.wikihow.com/Find-the-IMEI-or-MEID-Number-on-a-Mobile-Phone
- Identidad internacional de equipo móvil (IMEI): https://es.wikipedia.org/wiki/IMEI
- Identidad Internacional de Suscripción al Servicio Móvil (IMSI): https://es.wikipedia.org/wiki/IMSI

El sitio de Yo y Mi Sombra de Tactical Tech contiene muchas guías sobre tecnología celular.

- Materiales descargables de Yo y Mi Sombra: https://myshadow.org/materials
- Sitio de Yo y mi Sombra: https://myshadow.org/es

image-1605452256072.png
Image not found or type unknown

Revision #6
Created 26 April 2023 00:27:40 by Kira
Updated 28 July 2023 15:03:53 by Kira