Estudio de Caso:

ACOSO Y AMENAZAS

INSTITUTE FOR
WAR & PEACE REPORTING

IWPR

CASO

Al **trabajar** en la **defensa** de los **derechos sexuales y reproductivos** estoy acostumbrada a cierta resistencia en algunas audiencias. **Me habían cuestionado sobre mi trabajo**, sobre todo el tema del **aborto**, pero nunca había percibido que hubiera cierta organización en los **ataques** y que todos fueran **dirigidos hacia mi** y no a la temática en general, por lo que mi reacción inicial, cuando **empecé a recibir sin parar mensaje tras mensaje**, luego de días de ser **atacada en las redes sociales**, fue la de adoptar un bajo perfil y esperar a que bajara el nivel de agresiones, lo cual fue **muy estresante.**

"Antes recibías la amenaza,
un mensajito, una piedra en la ventana, y estaban tus compañeras para defenderte.
Ahora no.
Recibes el **mail** o el **tuit** y estás sola y dices **¿Qué hago?** Aunque estoy en un mundo de gente conectada, estoy sola para hacer frente a esto".

DEFENSORA

Una activista en favor de los derechos sexuales en un país en el que las leyes se han modificado, pero el contexto es muy conservador.

PRESUNTO AGRESOR
IDENTIFICADO POR LA DEFENSORA

Grupos en contra de la defensa de los derechos sexuales y reproductivos de la mujer.

¿Cómo se sintió frente al ataque?
Exhibida, perseguida, humillada y muy censurada.

¿Qué hizo ante el ataque?
Me autocensuré y pasé mucho estrés.

¿Qué hubiera hecho diferente?
Documentar el ataque, control de crisis e informarme sobre las posibilidades de denuncia.

RECOMENDACIONES

- **Que los gobiernos reconozcan las violencias en el mundo digital y la urgencia de generar leyes que garanticen seguridad para las ciudadanas y activistas**
- **Acudir a redes de mujeres que dan apoyo psicosocial**
- **Revisar las opciones de denuncia en las redes sociales como las de Twitter**
- **Hacer una documentación de los ataques**
- **Activar la verificación de dos pasos en cuanto se presente una situación similar**

** Estas fichas se realizaron con la revisión de entrevistas y cuestionarios realizados a 13 mujeres defensoras de derechos humanos de América Latina, que participaron en un proceso de formación en seguridad digital. La información de la ficha se ha recopilado con base en cada uno de los instrumentos aplicados por IWPR buscando resguardar la identidad de las mujeres defensoras.

Estudio de Caso:

PHISHING (ROBO DE INFORMACIÓN)

INSTITUTE FOR WAR & PEACE REPORTING

IWPR

CASO

Me **enviaron un correo** al trabajo con un **archivo confidencial de un caso** al que yo daba seguimiento y **para abrirlo me volvía a pedir la clave de mi correo**, en realidad **yo misma entregué** a mi **agresor** las **claves** para **acceder a mi información.** Sin que yo me diera cuenta, **él veía datos que sólo yo podía conocer,** y esos mismos datos aparecían publicados en redes. No entendía qué pasaba, **perdí la confianza** de personas clave en el equipo, **pensé que había personas infiltradas,** hasta que **pedí asesoría** y descubrieron que toda la información de mi correo estaba siendo **revisada en silencio por alguien más.**

"Te sientes **desnuda** cuando algo así sucede sucede y **culpable** por haber **desconfiado** de las compañeras."

¿Qué hubiera hecho diferente?
No hubiera regalado mi clave en una página falsa diseñada para parecerse a la de mi organización, hubiera sido más cuidadosa y les habría puesto más difícil conseguir mi clave. Habría cambiado mensualmente mis claves, y usado la verificación de dos pasos.

DEFENSORA

Una mujer que lleva años en la defensa del territorio de un país donde empresas transnacionales han avanzado con su depredación.

PRESUNTO AGRESOR
IDENTIFICADO POR LA DEFENSORA

Grupo organizado interesado no sólo en robar información, sino en vigilar su trabajo durante varios meses

¿Cómo se sintió frente al ataque?
Exhibida, perseguida, humillada y culpable por haber desconfiado de mis compañeras.

¿Qué hizo ante el ataque?
Primero no hice nada, porque ni siquiera sabía que había sido víctima de un ataque. Cuando todo se volvía más extraño y busqué asesoría, seguí los consejos de las personas que descubrieron que estaba siendo atacada. dijeron que cambiara las claves y me recomendaron tomar un curso de seguridad digital.

RECOMENDACIONES

- **Siempre verifica el remitente de tus correos electrónicos o mensajes en celulares. Nunca abras un link o descargues un archivo adjunto hasta verificar esa información**
- **Introduce tus datos solamente en páginas certificadas con "https", desconfía de todo lo que te aparezca como un pop up o página emergente.**
- **Usa la verificación de dos pasos en tu correo electrónico**
- **El phishing está diseñado para asemejarse a correos o comunicaciones que podrían parecerte verdaderas, de manera que caigas y puedan obtener tus credenciales de alguna plataforma, verifica que lo sitios que visitas sí sean los reales**
- **Dialoga abiertamente con tus compañerxs en el trabajo, sobre todo si ocurre algo extraño**

** Estas fichas se realizaron con la revisión de entrevistas y cuestionarios realizados a 13 mujeres defensoras de derechos humanos de América Latina, que participaron en un proceso de formación en seguridad digital. La información de la ficha se ha recopilado con base en cada uno de los instrumentos aplicados por IWPR buscando resguardar la identidad de las mujeres defensoras.

Estudio de Caso:

ROBO DE IDENTIDAD

INSTITUTE FOR WAR & PEACE REPORTING

IWPR

CASO

Con la **intención de dañarme** y **desprestigiarme**, **abrieron perfiles de Facebook y Twitter con mis fotos y datos personales. Primero pensé** que podría ser **una broma** de mal gusto de alguna persona conocida pero cuando vi las publicaciones **me di cuenta** de que eran **amenazas hacia mí y un riesgo para mis seres queridos.**

"Hay una **falta de conciencia** de que nos encontramos en una **situación de riesgo.** Es como un **mecanismo de protección** que te hace decir: **'si no lo veo no existe, mejor digo que no hay un riesgo y no tomo ninguna medida'**. O simplemente te lo tomas a la ligera y dices:'no pasa nada, a nosotras no nos va a pasar"

DEFENSORA

Activista que documentaba casos de violaciones a derechos humanos en Latinoamérica.

PRESUNTO AGRESOR
IDENTIFICADO POR LA DEFENSORA

Alguien de su entorno.

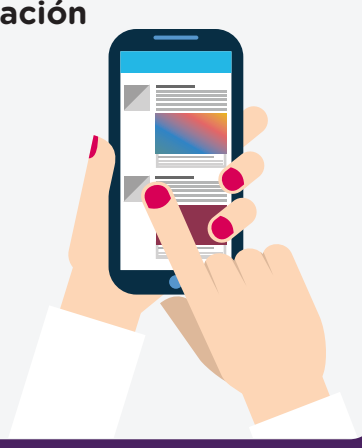
¿Cómo se sintió frente al ataque? Confundida y acosada.

¿Qué hizo ante el ataque?
Adopté un perfil bajo y di de baja mis redes sociales. Avisé a mis amistades y personas conocidas. No sabía que más podía hacer.

¿Qué hubiera hecho diferente?
Habría documentado el ataque y denunciado como amenaza, ahora sé que en algunos países esto es ilegal y puede servir de antecedente. Sé que es difícil pero ahora tendría más elementos y personas con las que asesorarme. Desde antes habría tenido todas las precauciones con respecto a la información que estaba compartiendo para no facilitar que me pudieran robar la identidad, aunque entiendo que esta es una decisión muy personal.

RECOMENDACIONES

- **Realizar sesiones de autodoxeado donde busques y revises qué información está disponible de ti en línea y quienes pueden tener acceso a tu información en redes sociales, por ejemplo**
- **Revisar las configuraciones de seguridad de tus redes para que tengas control total de tu contenido en las plataformas**



** Estas fichas se realizaron con la revisión de entrevistas y cuestionarios realizados a 13 mujeres defensoras de derechos humanos de América Latina, que participaron en un proceso de formación en seguridad digital. La información de la ficha se ha recopilado con base en cada uno de los instrumentos aplicados por IWPR buscando resguardar la identidad de las mujeres defensoras.

Estudio de Caso:

BAJA DE PERFIL FACEBOOK - EXPOSICIÓN DE VERDADERA IDENTIDAD ANTE PLATAFORMA DE RED SOCIAL

INSTITUTE FOR WAR & PEACE REPORTING

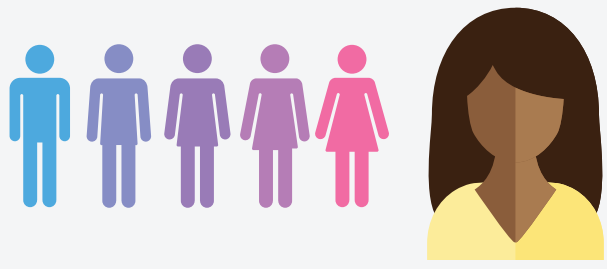
IWPR

CASO

Después de u**na campaña en redes** que **comencé a impulsar desde Facebook para denunciar acoso por parte de un servidor público**, comencé a recibir **correos de desconocidos que me hacían preguntas pretendiendo querer conocerme y ser mis amigos. Nunca respondí a ninguna solicitud** pero **después de unos días encontré mi cuenta suspendida** por "infringir las normas comunitarias de Facebook".

Dejé que mi cuenta quedara suspendida **y cuando quise regresar a la red social**, Facebook me notificó que **debía verificar mi identidad.** Para recuperar mi cuenta entregué a Facebook mi pasaporte (hasta ahora no he sido notificada de qué hizo con mi información). Cuando pudo verificar que yo era la dueña de la cuenta, me pidió poner mi nombre completo y real en mi perfil. Debido a mi trabajo y para proteger mi identidad, usaba un nombre falso y después de los ataques recibidos no iba a permitir que publicaran mi nombre real. **Así que hasta hoy casi a dos años, sigo sin Facebook.**

DEFENSORA



Mujer dedicada a la defensa de los derechos políticos de los grupos de mujeres y LGBT

PRESUNTO AGRESOR
IDENTIFICADO POR LA DEFENSORA

Un político o política o una institución pública

¿Cómo se sintió frente al ataque?
Indignada, enojada y confundida.

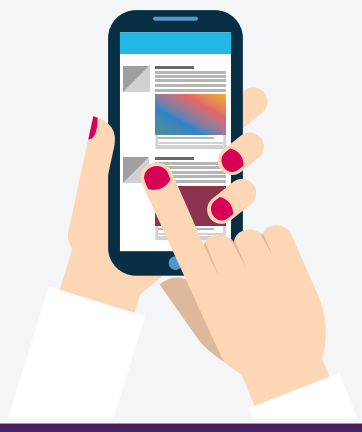
¿Qué hizo ante el ataque?
No volví y no volvería a esa red social que prefiere proteger a atacantes que a defensoras.

¿Qué hubiera hecho diferente?
Habría contactado a las compañeras que acompañan estos casos para que el mío pudiera ser documentado y denunciado, eso sí, jamás tendré un perfil con mi verdadero nombre, pongo en riesgo mi seguridad e integridad, eso no lo cambiaré.

RECOMENDACIONES

- **Las plataformas de redes sociales deben poder diferenciar y atender los ataques a las activistas, defensoras y víctimas de acoso**
- **Las plataformas de redes sociales deben aclarar el uso que hacen con la información personal**
- **Activistas y defensoras deben tener el derecho de resguardar su identidad por condiciones de seguridad**
- **Prepararse y antes de lanzar una campaña en redes sociales, considerar activar un pequeño protocolo, previendo que otro tipo de ataques se pueda presentar, como activar momentáneamente la verificación de dos pasos en caso de que no se use aún**

"Pareciera que si no tienes Facebook, no existes. Movimientos y acciones se organizan en la red social; comunicaciones no solo de activismo sino personales también las perdí al dejar ese espacio. **Lo peor no es no tener Facebook sino no saber qué hizo con mi información oficial."**



** Estas fichas se realizaron con la revisión de entrevistas y cuestionarios realizados a 13 mujeres defensoras de derechos humanos de América Latina, que participaron en un proceso de formación en seguridad digital. La información de la ficha se ha recopilado con base en cada uno de los instrumentos aplicados por IWPR buscando resguardar la identidad de las mujeres defensoras.

Estudio de Caso:

ALLANAMIENTO DE INSTALACIONES

INSTITUTE FOR WAR & PEACE REPORTING

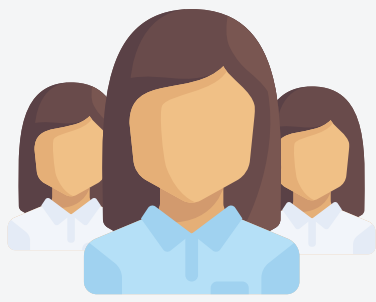
IWPR

CASO

Entraron por la noche mientras no había nadie en la oficina, no sabemos cuántas personas eran pero asumimos que más de una, pues **se llevaron todos los equipos de trabajo, nada de dinero. Solamente computadoras y un par de teléfonos** que tenemos en escritorios para cuando hacemos salidas a terreno. La entrada estaba forzada. **Lo que más nos preocupa es pensar en toda la información que se llevaron, los datos de las personas que defendemos estaban en esos equipos. Sus teléfonos, direcciones y detalles sobre sus casos.** No tenemos un protocolo para manejar esa información con mayor sensibilidad. Hace mucho tuvimos una capacita ción digital para proteger y enviar información delicada. Supongo que no habíamos contemplado la posibilidad de que al robarte un equipo te roban toda la información en él.

"Hemos tenido que **tomar medidas de seguridad**, con instalación de cámaras, si no conoces a la persona no abres hasta saber las intenciones que trae, **no podemos confiar en nadie**"

DEFENSORA



Grupo de defensoras dedicadas a la defensa jurídica de mujeres sobrevivientes de violencia

PRESUNTO AGRESOR
IDENTIFICADO POR LA DEFENSORA

Grupo de detractores al trabajo en defensa de las mujeres

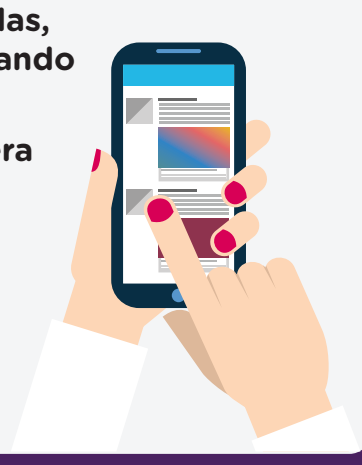
¿Cómo se sintió frente al ataque?
Sensación de vulnerabilidad, impotencia ante la impunidad e incertidumbre con respecto a los motivos del ataque.

¿Qué hizo ante el ataque?
Fue impactante saber que habían estado ahí, y ver que ya no estaba todo nuestro trabajo y la información de las y los beneficiarios. Denunciamos por robo. Informamos a una de las financiadoras y vimos la opción de poder comprar al menos un equipo para reponer uno de los sustraídos y buscamos una copia de seguridad que habíamos hecho, que aunque no tenía toda la información al menos sí nos permitía recuperar lo suficiente para regresar al trabajo con cierta normalidad.

¿Qué hubiera hecho diferente?
"Hubiéramos contactado con las víctimas y sus familiares, pues su información quedó comprometida, para informarles lo ocurrido y analizar los riesgos en que esta situación los coloca. Realización de evaluaciones de riesgo de cada uno de los casos ante el nuevo escenario con organizaciones expertas. Presentación de la denuncia como ataque a personas defensoras, identificando el delito más allá del "robo común". Habríamos resguardado toda la información y claves en las computadoras y celulares para que al llevarse los equipos no la pudieran extraer."

RECOMENDACIONES

- **Haz un ejercicio con el equipo sobre los tipos de información que deberían de respaldar, incluyan los contactos y establezcan a nivel organizacional cada cuánto se hará el respaldo**
- **Procura hacer respaldos periódicos de tu información**
- **Considera cifrar los discos duros donde almacenes tus respaldos**
- **No guardes ese respaldo en la oficina, llévalo a otro lugar y, periódicamente, ese lugar puede ir cambiando**
- **Cifra los equipos y dispositivos móviles, utiliza una contraseña segura y recuerda apagar los equipos cada día. Muy pocos teléfonos celulares pueden fallar durante el cifrado, recuerda que únicamente debes hacerlo una vez para activarlo, pero tu teléfono debe estar conectado todo el tiempo durante el proceso y te recomendamos que realices un respaldo antes de hacerlo**
- **En caso de los teléfonos móviles que se utilizan durante los viajes puedes decidir formatearlos después de cada viaje o borrar las conversaciones, llamadas, multimedia y contactos que hayan almacenado durante el viaje, notificando antes de hacerlo a lxs miembros de la organización**
- **Las cámaras de seguridad son muy buena medida, únicamente considera si sería mejor alojar las grabaciones en las mismas instalaciones o tenerlas en línea**



** Estas fichas se realizaron con la revisión de entrevistas y cuestionarios realizados a 13 mujeres defensoras de derechos humanos de América Latina, que participaron en un proceso de formación en seguridad digital. La información de la ficha se ha recopilado con base en cada uno de los instrumentos aplicados por IWPR buscando resguardar la identidad de las mujeres defensoras.

Estudio de caso:

ATAQUE AL SERVIDOR DE LA ORGANIZACIÓN

INSTITUTE FOR WAR & PEACE REPORTING

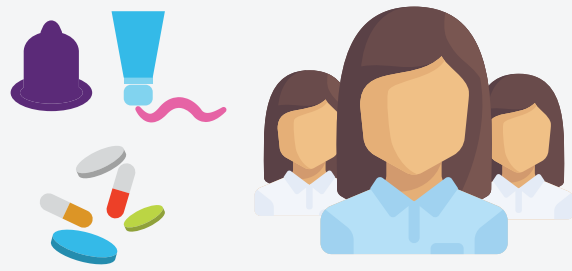
IWPR

CASO

De manera remota **(la verdad no sé cómo lo lograron) nos hackearon equipo de cómputo y, al hacerlo, entraron a nuestras carpetas en Dropbox.** De esta manera, alcanzaron tres computadoras, a **una de ellas la dejaron totalmente inservible y de las otras logramos rescatar gran parte de la información. Durante ese mismo ataque, uno de los servidores fue infectado o dañado, y la información que contenía fue cifrada.**

"Se **invierte menos tiempo cuando previenes** que cuando sufres un ataque que además daña la imagen de la organización."

DEFENSORA



Defensoras dedicadas la promoción de la salud sexual y reproductiva de personas jóvenes

PRESUNTO AGRESOR
IDENTIFICADO POR LA DEFENSORA

Un grupo conservador con recursos económicos

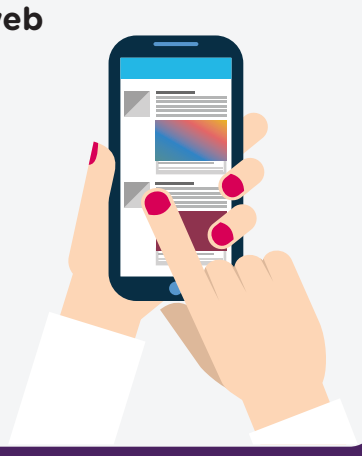
¿Cómo se sintió frente al ataque?
No fuimos muy conscientes. La verdad no le dimos importancia, por que rescatamos información de las computadoras y desconocíamos las implicaciones.

¿Qué hizo ante el ataque?
No entendimos la magnitud del ataque.

¿Qué hubiera hecho diferente?
Contaría con un servidor distinto, hubiéramos encriptado información para protegerla mejor.

RECOMENDACIONES

- **Documentar los ataques cuando suceden permite tomar mejores decisiones para solucionar y prevenir nuevos ataques. Así no se pierde ningún detalle del ataque**
- **Previo a lanzamientos de campañas, considerar el uso de herramientas como Deflect y verificación de dos pasos en redes sociales, cuentas de correo y sitio web**
- **Mejorar las contraseñas en nuestros servicios de nube**
- **Aprópiate de la tecnología y de tus equipos electrónicos**



** Estas fichas se realizaron con la revisión de entrevistas y cuestionarios realizados a 13 mujeres defensoras de derechos humanos de América Latina, que participaron en un proceso de formación en seguridad digital. La información de la ficha se ha recopilado con base en cada uno de los instrumentos aplicados por IWPR buscando resguardar la identidad de las mujeres defensoras.

Estudio de Caso:

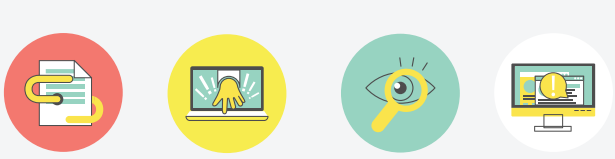
ATAQUES A IDENTIDAD PERSONAL Y PROFESIONAL (DESPRESTIGIO)

INSTITUTE FOR WAR & PEACE REPORTING

IWPR

CASO

Estábamos **a punto de lanzar nuestro reporte sobre abusos y violaciones a derechos humanos** y días antes,la noticia éramos nosotras. Salieron declaraciones públicas en radio, periódicos y redes sociales de miembros del Gobierno que decían: esta organización, esta persona, dijo esto, hizo eso. **Solo los aspectos negativos. Colocaron a la opinión pública en nuestra contra y desprestigiaron la credibilidad del trabajo.** El atacante ponía las palabras negativas pero cualquiera podía repetir lo que una autoridad estaba promoviendo.



"**A ningún gobierno le gusta que le digan que está haciendo las cosas mal y estamos en esa mira, porque ese es el trabajo en derechos humanos:** estar pendiente que lo que estás haciendo lo estés haciendo bien y en función de la sociedad, entonces allí es donde seríamos más vulnerables."

DEFENSORA

Defensora que trabaja en una organización para la promoción y defensa de los derechos humanos en su país

PRESUNTO AGRESOR
IDENTIFICADO POR LA DEFENSORA

El gobierno del país

¿Cómo se sintió frente al ataque?
Enojo al leer o escuchar las calumnias y mucha impotencia pues sabía que lo estaban haciendo para amedrentarme pero que desafortunadamente la gente escucha a quien tiene más poder. Me sentí muy desamparada.

¿Qué hizo ante el ataque?
Adoptando un bajo perfil, cerré mis cuentas de redes sociales y acudí a una red de apoyo de mujeres que trabajamos en Derechos Humanos por consejo. Algunas de ellas me recomendaron con expertos en seguridad digital.

¿Qué hubiera hecho diferente?
Hubiera documentado el ataque e indagado para descubrir a los responsables. Los responsables de lanzar las informaciones eran personas identificables que pudimos haber denunciado. Me hubiera mantenido en control. Hubiéramos realizado una campaña para fortalecer nuestra imagen y credibilidad apoyándonos en la red de apoyo y aliados nacionales e internacionales, hubiéramos pedido medidas de reparación por las difamaciones recibidas.

RECOMENDACIONES

- **Realizar una documentación de la agresión**
- **Denunciar o reportar el acoso a organizaciones a las redes sociales para que borren los comentarios**
- **Tejer redes de confianza y seguridad con las que puedas hablar de este tipo de situaciones y puedan ser tu soporte emocional**
- **No permitas que otros te hagan dudar de ti ni de tu trabajo**

** Estas fichas se realizaron con la revisión de entrevistas y cuestionarios realizados a 13 mujeres defensoras de derechos humanos de América Latina, que participaron en un proceso de formación en seguridad digital. La información de la ficha se ha recopilado con base en cada uno de los instrumentos aplicados por IWPR buscando resguardar la identidad de las mujeres defensoras.