

# Estudio de Caso:

## ACOSO Y AMENAZAS

### 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”.

## INSTITUTE FOR WAR & PEACE REPORTING



### 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



# Case Study:

## HARASSMENT AND THREATS

### CASE

“Working to defend sexual and reproductive rights means I’m used to resistance from some audiences, especially on the subject of abortion, but I had never felt that the attacks were organized or that they were directed against me personally. So, when I started to receive aggressive message after message, non-stop, for days on social networks, my initial reaction to being attacked was to adopt a low profile and wait for the aggression to stop; this was very stressful.”



“Before you’d get a threat, a message, a stone [thrown] at your window and you had your colleagues to defend you. Now you don’t. You get an **email** or a **tweet** and you’re on your own and you say ‘**what should I do?**’ Even though I’m in a world of connected people, I’m alone against this.”

## INSTITUTE FOR WAR & PEACE REPORTING



### DEFENDER



An activist defending sexual rights in a country where the laws have changed but the context remains very conservative

### SUSPECTED PERPETRATOR ACCORDING TO THE DEFENDER

Groups against the defense of the sexual and reproductive rights of women



#### How did the attack make you feel?

Exposed, hunted, humiliated and very censored.

#### How did you respond to the attack?

With self-censorship and stress.

#### What would you have done differently?

find out how to report it. Talk with my support network.



## RECOMMENDATIONS

- Ask governments to recognize violence in the digital world and the urgency of creating laws that guarantee citizens and activists' safety
- Join networks of women who provide psychosocial support
- Check options for reporting complaints in social networks such as Twitter
- Document the attacks
- Activate two-step verification when a similar situation happens



# Estudio de Caso: PHISHING (ROBO DE INFORMACIÓN)

## 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 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.



## RECOMENDACIONES

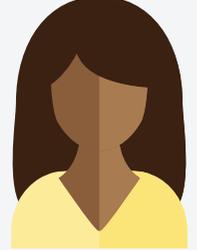
- Siempre verifica el remitente de tus correos electrónicos o mensajes en celulares. Nunca abras un link o descargues un archivo adjunto hasta verificar esa información
- Introduce tus datos solamente en páginas certificadas con "https", desconfía de todo lo que te aparezca como un pop up o página emergente.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

## INSTITUTE FOR WAR & PEACE REPORTING



## 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

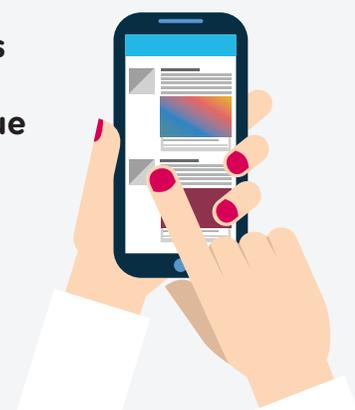


### ¿Cómo se sintió frente al ataque?

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.



# Case Study:

## PHISHING (INFORMATION THEFT)

### CASE

“I received an email to work with a confidential file for a case that I was working on. To open it I had to enter my email password again. By doing so, I gave my attacker my password to access my information. Without realizing he saw information that only I could know and he published it on networks. I didn't understand what was happening. I stopped trusting key people in the team. I thought that there were the moles until I sought advice and it was discovered that all of the information in my email was being read silently by someone else.”



“When something like that happens it makes you feel like you've been **stripped** and also **guilty** for not having **trusted** colleagues.”

**What would you have done differently?**  
Be more careful to avoid writing passwords into a false page. Change passwords every month and consider using two-step verification.



### RECOMMENDATIONS

- Always check who is sending you emails or messages to your phone. Never open a link or download a file until you have verified the source
- Only put your information into certified pages with “https;” don't trust anything that appears in a pop up
- Use two-step verification for your email
- Phishing is designed to look like emails and communications that could be real so that you trust it; always check that the websites that you visit are legitimate
- Speak openly with your colleagues about anything strange that is happening

Note: These case studies are based on interviews and questionnaires of 13 Latin American women human rights defenders who participated in a digital security training process. The information has been compiled based on the instruments applied by IWPR to ensure the protection of the women defenders' identities.

## INSTITUTE FOR WAR & PEACE REPORTING



### DEFENDER



A woman who has spent many years defending the land rights in a country that is being pillaged by transnational companies

### SUSPECTED PERPETRATOR ACCORDING TO THE DEFENDER

An organized group interested in both stealing information and monitoring her work for several months



#### How did the attack make you feel?

Exposed, hunted, humiliated and guilty for not having trusted my colleagues.

#### How did you respond to the attack?

At first I didn't do anything because I didn't even realize that I had been the victim of an attack. When things got even stranger, I sought advice and I followed the recommendations of the people who discovered that I was being attacked. They said that I should change my passwords and recommended that I take a course on digital security.



# Estudio de Caso:

## ROBO DE IDENTIDAD

### 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'"

#### ¿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.

## INSTITUTE FOR WAR & PEACE REPORTING



### 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.

# Case Study:

## IDENTITY THEFT

### CASE

They opened Facebook and Twitter profiles with my photos and personal information to cause harm and smear my reputation. At first I thought it was a bad joke by someone I knew, but when I saw the publications I realized that they were a threat to me and a danger to my loved ones.



"There isn't enough awareness that we're in a context of risk. It's like a defense mechanism that makes you say: 'If I can't see it, it doesn't exist; it's better to say there's no risk and not take any measures. 'Or you just don't take it seriously and say: 'It's OK; it won't happen to us.'"

#### What would you have done differently?

Document the attack and report it as a threat. Look for resources and people to provide advice. Check the privacy configuration of my online profiles to make sure I feel comfortable with the information I am sharing online.



### RECOMMENDATIONS

- Conduct regular online searches using your name to review the information that is publicly available about you online and in your social networks
- Check the safety configurations in your networks so that you have complete control over the contents on the platforms

## INSTITUTE FOR WAR & PEACE REPORTING



### DEFENDER



An activist who documents cases of human rights violations in Latin America

### SUSPECTED PERPETRATOR ACCORDING TO THE DEFENDER

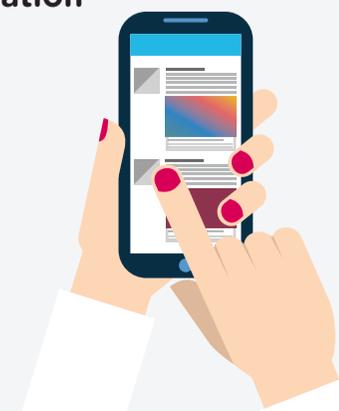
Someone in her surroundings



How did the attack make you feel?  
Confused and harassed.

#### How did you respond to the attack?

I adopted a low profile and took down my social networks. I told my friends and acquaintances. I didn't know what else I could do.



# Estudio de Caso:

## BAJA DE PERFIL FACEBOOK – EXPOSICION DE VERDADERA IDENTIDAD ANTE PLATAFORMA DE RED SOCIAL

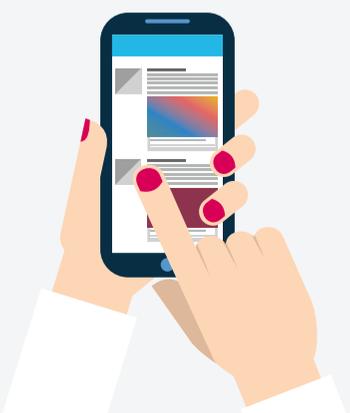
### CASO

Después de una 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.



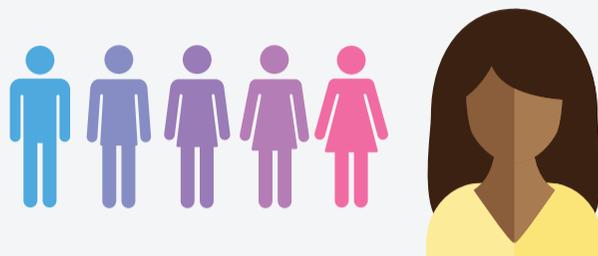
“Pareciera que si no tienes Facebook, no existes. Movimientos y acciones se organizan en la red social; comunicaciones no solo de activismo sino personales también las perdí al dejar ese espacio. Lo peor no es no tener Facebook sino no saber qué hizo con mi información oficial.”



## INSTITUTE FOR WAR & PEACE REPORTING



### 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

\*\* 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.

# Case Study:

## FACEBOOK PROFILE DEACTIVATION – EXPOSURE OF REAL IDENTITY TO THE SOCIAL NETWORK PLATFORM

### CASE

After a campaign on social networks, including Facebook, in which I denounced harassment committed by a public servant, my account was suspended for “violating Facebook’s Community Standards.”

When I wanted to return to the social network, Facebook informed me that I needed to verify my identity. To recover my account, I gave Facebook a scan of my passport (I still have not been informed about what they did with my information).

Once they had verified that I owned the account, they asked me to put my real full name on the account. I had used a false name because of my activism work and to protect my identity, and after the attacks I wasn’t going to allow my real name to be made public. So now, nearly two years on, I still don’t have Facebook.

## INSTITUTE FOR WAR & PEACE REPORTING



### DEFENDER



A woman who defends the political rights of women and LGBT

### SUSPECTED PERPETRATOR ACCORDING TO THE DEFENDER

A politician or a public institution



**How did the attack make you feel?**  
Annoyed, angry and confused.

**How did you respond to the attack?**

I have not and will not go back onto this social network, which prefers to protect attackers than human rights defenders.

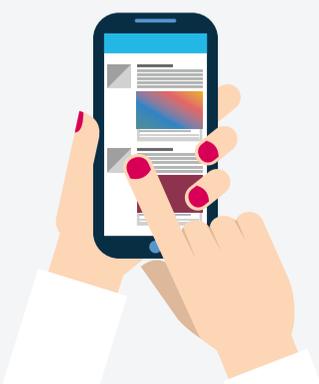
**What would you have done differently?**

Contact colleagues or groups that follow cases so that this case can also be documented and reported. Consider if having a profile with my real name in that platform could put my security and integrity at risk.



## RECOMMENDATIONS

“It seems like you don’t exist if you don’t have Facebook. Movements and actions are organized on social networks. I not only lost communications about activism but also personal ones when I stopped using the space. However, the worst thing for me is not knowing what they did with my official information.”



- Social network platforms should be able to differentiate and deal with attacks against activists, human rights defenders and victims of harassment
- Social network platforms should explain what they do with your personal information
- Activists should prepare themselves before launching a campaign on a social network. Think about potential attacks that could take place, and implementing a protocol to prevent to mitigate them
- Learn how to implement two-step verification temporarily, if you’re not already using it all the time.

# Estudio de Caso:

## ALLANAMIENTO DE INSTALACIONES

### 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 capacitación 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**"

#### ¿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 los 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



## INSTITUTE FOR WAR & PEACE REPORTING



### 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.

# Case Study:

## BREAKING AND ENTERING A BUILDING

### CASE

They entered at night when no one was at the office. We assume that there was more than one person, because they took all our work equipment. They didn't take any money, just computers and a couple of telephones that we had on desks for when we go out in the field. The door had been forced open. What worries us most is thinking about all of the information they took, information about the people we defend was on that equipment, their telephone numbers, addresses and details about their cases.



"We've had to take security measures, we've installed cameras. If you don't know the person don't open the door until you know what they want. We can't trust anyone."

## INSTITUTE FOR WAR & PEACE REPORTING



### DEFENDER



A group providing legal defense for women survivors of violence

### SUSPECTED PERPETRATOR ACCORDING TO THE DEFENDER

A group of people against their work defending women



**How did the attack make you feel?**  
Vulnerable, powerlessness against the impunity and uncertainty about the motive for the attack.

#### What did you respond to the attack?

It was shocking to know that they had been there and to know that all our work and information about the beneficiaries was gone. We reported the robbery. We informed one of our funders and saw how we could buy at least one computer to replace the stolen ones and we found a backup copy we'd made. Although it didn't have all the information on it, at least it gave us the chance to recover enough to go back to work with some normality.

#### What would you have done differently?

Contact the victims and their families because their information had been compromised, to let them know what happened and analyze the risks resulting from this situation. Implement risk evaluations for each case considering the new circumstance with expert organizations. Report that the attack was made against human rights defenders to identify that the crime was more than a "common robbery." Protect all of the information and use passwords on the computers and cell phones so it they can not be accessed in case the equipment is taken."



## RECOMMENDATIONS

- Carry out a team exercise on the types of information and contacts that should be backed up and establish how often they will be backed up at an organizational level
- Ensure you make periodic backups of information
- Consider encrypting the hard drives where backups are stored
- Store the backup off-site and regularly change the location where it is stored
- Encrypt equipment and mobile devices, use a secure password and remember to turn off the equipment daily when you leave the office. When you encrypt your phone, remember it must be connected and plugged in during the whole process and we recommend making a backup beforehand.
- Mobile phones used on sensitive trips or meetings can be reformatted after each occasion. Alternatively delete the conversations, calls, multimedia and contacts that you stored during the trip (informing members of the organization before doing so)
- Install security cameras but don't keep the server or store the videos in the same office; configure the security cameras so that storage is online.



# Estudio de caso:

## ATAQUE AL SERVIDOR DE LA ORGANIZACIÓN

### 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.

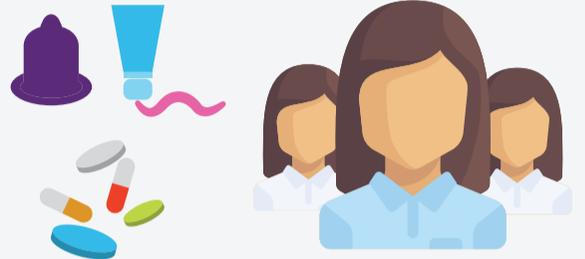


"Se invierte menos tiempo cuando previenes que cuando sufres un ataque que además daña la imagen de la organización."

## INSTITUTE FOR WAR & PEACE REPORTING



### 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.

# Case Study:

## ATTACK ON THE ORGANIZATION'S SERVER

### CASE

We were hacked, we don't really know how. They went inside our Dropbox files. They reached three computers; one of them was left destroyed, yet we were able to recover most of the information from the other two. During this same attack, one of the servers ended up infected or damaged and information it contained was ciphered.

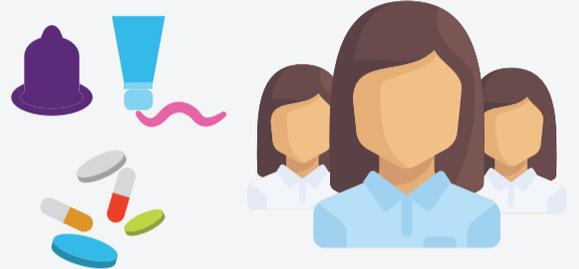


"Less time is invested when you prevent than when you suffer an attack. Besides, it also affects the organization's image."

## INSTITUTE FOR WAR & PEACE REPORTING



### DEFENDER



Woman who promotes sexual and reproductive health of young people.

### SUSPECTED PERPETRATOR ACCORDING TO THE DEFENDER

A conservative group with economic resources.



#### How did the attack make you feel?

In truth, we didn't think it was so important, as we could rescue most of the information from the computers and we ignored the implications.

#### What did you respond to the attack?

We didn't understand the magnitude of the attack.

#### What would you have done differently?

We would have a different server with encrypted information for better protection.



## RECOMMENDATIONS

- Documenting the attacks as soon as possible allows you to make better decisions to resolve the problem and prevent new attacks. In this way, no detail about the attack is lost
- Before launching campaigns, consider using tools such as Deflect and the two-step verification on social media, email accounts and webpages.
- Improve passwords in the cloud's services.
- Take possession of the technology and your electronic equipment.



Note: These case studies are based on interviews and questionnaires of 13 Latin American women human rights defenders who participated in a digital security training process. The information has been compiled based on the instruments applied by IWPR to ensure the protection of the women defenders' identities.

# Estudio de Caso:

## ATAQUES A IDENTIDAD PERSONAL Y PROFESIONAL (DESPRESTIGIO)

### 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."

#### ¿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.

## INSTITUTE FOR WAR & PEACE REPORTING



### 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.

