Case Study:
HARASSMENT AND THREATS

INSTITUTE FOR
WAR & PEACE REPORTING

IWPR

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."

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**

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.

Case Study:

PHISHING (INFORMATION THEFT)

INSTITUTE FOR WAR & PEACE REPORTING

IWPR

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.

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

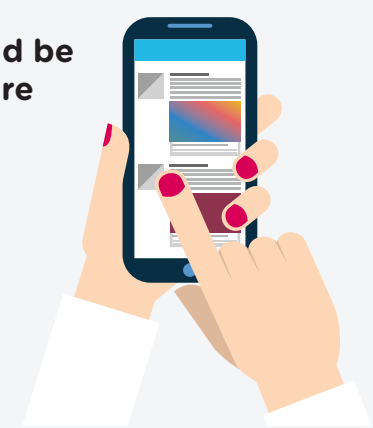
An organized group interested in both stealing information and monitoring her work for several months

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.

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.

Case Study:
IDENTITY THEFT

INSTITUTE FOR WAR & PEACE REPORTING

IWPR

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.'"**

DEFENDER

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

SUSPECTED PERPETRATOR
ACCORDING TO THE DEFENDER

Someone in her surroundings

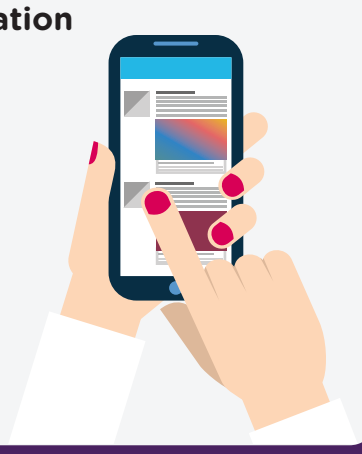
How did the attack make you feel?
Confused and harassed.

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.

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**



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.

Case Study:

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

INSTITUTE FOR WAR & PEACE REPORTING

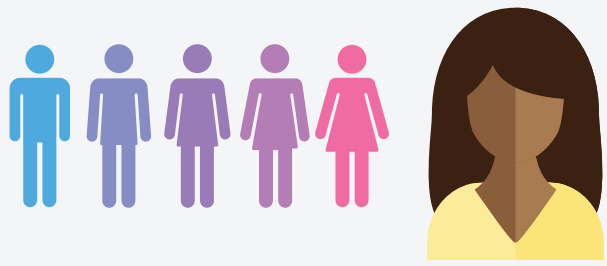
IWPR

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.

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.

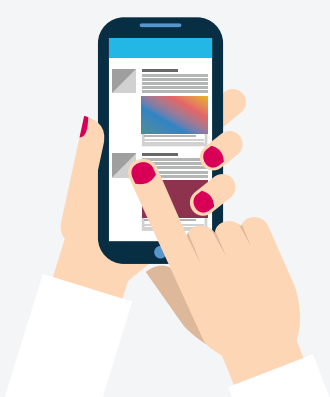
How did you respond to the attack?
I have not and will not go back onto this social network, which prefers to protect attackers than human rights defenders.

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.**

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.

Case Study:

BREAKING AND ENTERING A BUILDING

INSTITUTE FOR WAR & PEACE REPORTING

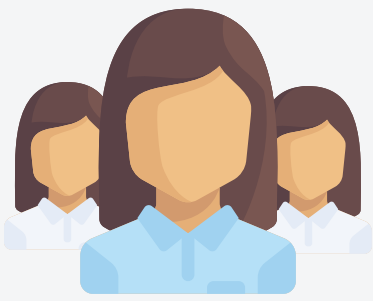
IWPR

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.**"

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

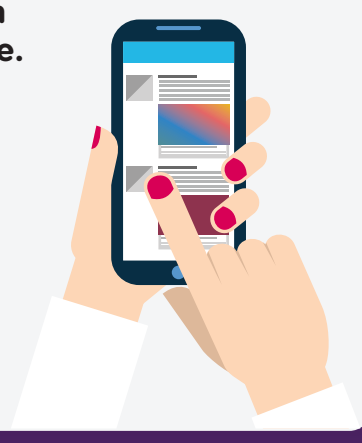
How did the attack make you feel?
Vulnerable, powerlessness against the impunity and uncertainty about the motive for the attack.

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.**



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.

Case Study:

ATTACK ON THE ORGANIZATION'S SERVER

INSTITUTE FOR WAR & PEACE REPORTING

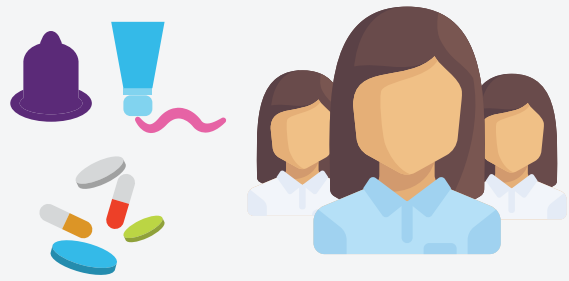
IWPR

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."

DEFENDER



Woman who promotes sexual and reproductive health of young people.

SUSPECTED PERPETRATOR
ACCORDING TO THE DEFENDER

A conservative group with economic resources.

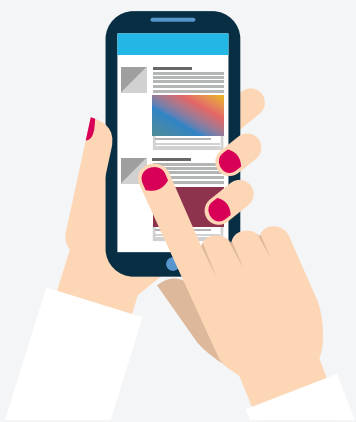
How did the attack make you feel?
In truth, we didn't think it was so important, as we could rescue most of the information from the computers and we ignored the implications.

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.