AFD AGENCE FRANÇAISE DE DÉVELOPPEMENT

Funded by the European Union

forus CONNECT SUPPORT INFLUENCE

INNOVUS

Security Digital and risk management

Session #2

We must take care of communications

2025

1. General Information

1. Course/workshop name: Introduction to Digital Security for Non-Governmental Organizations (NGOs) & Human Rights Defenders (HRDs)
2. Duration: maximum 115 minutes (in order to stay within this time frame, the facilitator may need to choose only some of the WhatsApp configuration settings from the last exercise)
3. Target audience: directors of NGOs and human rights organizations
4. Course objectives: To acquire basic knowledge of digital security to integrate into the daily practices of NGOs and human rights organizations, enabling them to strengthen their resilience and sustainability.

2. Preparation for facilitation

- Materials needed: The presentation and a reading. No prior knowledge is necessary, except for having completed the survey and reading a text. All other materials are included in the presentation.
- Space setup: Check the sound and image, and set up the projector screen.
- Support technologies: links, activities, and evaluation.
- Preparation prior to the session (logistics, review of materials): For this session, both the facilitator and the participants should have read the following article in advance: https://hipertextual.com/seguridad/estafa-wi-fi-gratuito-aeropuertos-robo-datos-personales/
- Step-by-step guide for each activity: found in each point
- Instructions on transitions between topics: These are marked in the presentation
- Critical points to emphasize: Always keep in mind that this is just a preview and that there is no such thing as 100% effective digital security.

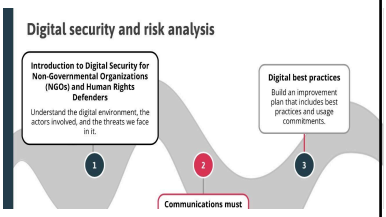
3. Script for session 2 (described slide by slide)

Minute 1.	**Activity/Action of the facilitator** Welcome and present course objectives	**Strategy/Methodology** Story about a generic visual
Script/instructions - Welcome to the course Introduction to Digital Security for Non-Governmental Organizations (NGOs) and Human Rights Organizations (HROs) - Facilitator's name: xxxxx - No prior knowledge is required to attend this session; you only need to have completed the baseline construction questionnaire. You should have received a reading to prepare, but if you did not, don't worry, you will understand it in context.		

Minute 2.	**Facilitator's activity/action**	**Strategy/Methodology**
	Introduction to the topic	Story about a generic visual

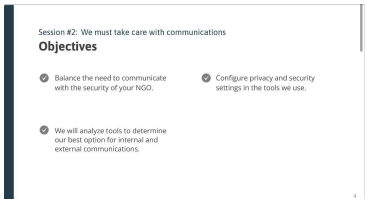
Script/instructions

- As we saw in the first session, digital security is a complex topic that we know something about, but almost no one can claim to have in-depth knowledge of. We will continue to approach the topic in a practical way to learn how to protect ourselves when we inhabit and use digital media.
- Remember that digital security aims to enable people to use technology safely, privately, and with confidence. Once again, a balanced view of digital security puts people at the center.
- Let 's get started!

Minute 3	**Facilitator activity/action**	**Strategy/Methodology**
	Introduction to the topic	Story about a descriptive visual

Script/instructions

- The objectives of the course are: to acquire basic knowledge of digital security to integrate into the daily practices of NGOs and human rights organizations, enabling them to strengthen their resilience and sustainability.
- I remind you that in this module we will approach digital security from a risk analysis perspective, and the specific idea of this second session is to think about the digital security of internal and external communications.
- Don't forget that in the third session we will focus on developing a basic plan that will enable you to improve your daily practices and thereby enhance your digital security.

Minute 4	**Facilitator activity/action**	**Strategy/Methodology**
	Introduction to the topic	Story about a descriptive visual

Script/instructions

- During this second session, we will focus on reflecting on how to balance the need to communicate with the security of your NGOs.
- We will take one of the tools most used by your organizations—according to the survey we conducted—to adjust its configuration settings and thus improve security and privacy. Ideally, you will then make an inventory of the tools you use and prioritize them in order to gradually repeat the exercise of adjusting the configuration settings with the main ones.

- At the end of this session, you will have tools to evaluate and identify the digital communication services you use most in your organization and will be able to identify the most common risks, threats, or vulnerabilities you face there.
- Although we will do the exercise with one tool, the idea is that at the end of the session you will be able to repeat the exercise with others that you use, in order to improve your security and privacy.

Minute 6	**Activity/Action by the facilitator**	**Strategy/Methodology**
	Introduction to the topic	Story about a descriptive visual

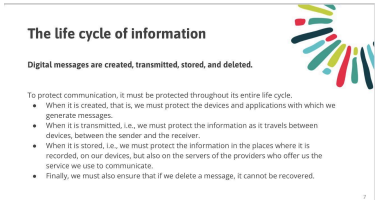
Script/instructions

- Digital technologies, especially cell phones, have facilitated communication in ways that were unthinkable just a couple of decades ago, shortening distances and enabling activities that were once perhaps a dream. We can no longer think about our personal or professional activities without mobile devices playing a role in them. However, the amount of personal information that these devices store about us (contacts, photos, documents, browsing and communication histories, for example) also makes us very vulnerable. If someone has access to our cell phone, they have access to a large amount of personal data and can learn many things about our lives.
- Protecting our communications and understanding the role of cell phones in this context is key to preventing communications surveillance or mitigating the risks of this activity.

Minute 7	**Facilitator's activity/action**	**Strategy/Methodology**
	Introduce the first topic of Session 1	Story about a generic visual

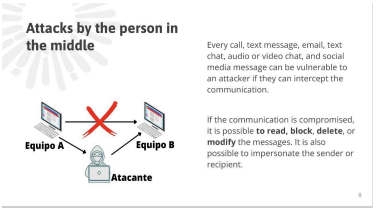
Script/instructions

- To address the digital security risks posed by the tools we use, as well as understanding that many intermediary companies are involved in the process, it is also key that we understand the life cycle of the information we manage. Let's take a closer look at this now

Minute 8	**Activity/Action by the facilitator**	**Strategy/Methodology**
	Explain the life cycle of information.	Narrative about a descriptive visual containing the text to be repeated. The slide describes four important moments in the information life cycle. The facilitator should emphasize each of these steps and differentiate between them.

Script/instructions

- *Read the slide*
- As we saw in the last session, the most frequent risks to civil society occur because there are also frequent attacks that exploit a series of vulnerabilities present in the digital environment. We are going to focus on the relationship between digital risks, vulnerabilities, and the types of attacks they enable. First, I will give you an example, and then we will do different activities.

Minute 10	**Activity/Action by the facilitator.**	**Strategy/Methodology**
	Provide an example of how information can be accessed irregularly in a specific modality, namely a "man-in-the-middle attack" that exploits vulnerabilities in public Wi-Fi networks during the data transfer process.	Narrative about a descriptive visual containing the text to be repeated.

Script/instructions

- One way to understand system vulnerabilities and how an attack can materialize a risk is to explain an example of an attack known as a "man-in-the-middle attack," which occurs during the information transmission phase.
- *Read the slide*
- Another way to understand this more clearly is with a practical example: A user connects to their bank from a public Wi-Fi network in an internet café. Another person, the attacker, connected to the same network, executes the man-in-the-middle attack, intercepting the connection between the user's browser and the bank's server. The user believes they are communicating directly with the bank, but in reality they are passing through the attacker's server, who can see and capture everything the user transmits.

Minute 15	**Activity/Action by the facilitator.**	**Strategy/Methodology**
	Facilitate a practical exercise with the course participants.	Story about a visual aid that seeks to illustrate

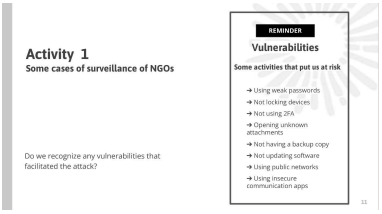
Script/instructions

- To better illustrate this type of risk, we will carry out an activity in which we will analyze a real example in which information obtained via public Wi-Fi was circulated.
- *Read the slide*
- *Give participants a few minutes to recall the details of the case and then proceed to analyze it collectively in light of the questions that appear on the slide as follows*:

Minute 18	**Activity/Action by the facilitator.**	**Strategy/Methodology**
	Facilitate a practical exercise with the course participants	Story about a visual aid that seeks to illustrate

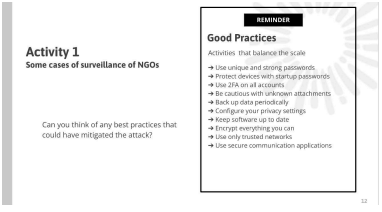
Script/instructions

- *Read the slide*
- What type of attack do we recognize?
  The facilitator asks the question and helps with the reminder, encouraging people to respond. They can do so via chat and discuss the answers. The facilitator should prepare for this session by reviewing the information provided in the previous session. The correct answer is phishing.

Minute 22	**Activity/Action by the facilitator.**	**Strategy/Methodology**
	Facilitate a practical exercise with the course participants	Story about a visual aid that seeks to illustrate the point.

Script/instructions

- *Read the slide*
  Do we recognize any vulnerabilities that facilitated the attack?
  The facilitator asks the question and, with the help of the reminder, encourages people to respond. They can do so via chat and discuss the answers. The correct answer is Using public networks and Using insecure communication applications

Minute 26	**Facilitator activity/action**	**Strategy/Methodology**
	Facilitate a practical exercise with the course participants.	Story about a visual aid that seeks to illustrate

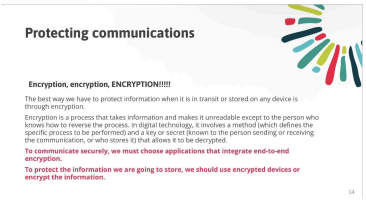
Script/instructions

- *Read the slide*
  Can you think of any good practices that could have mitigated the attack?
  The facilitator encourages people to respond, even via chat, and to discuss the responses. The correct answers are to use 2FA (two-factor authentication, the concept was covered in the first session) on accounts, to use only trusted networks, and to use secure communication applications.
  Additionally, you can recommend the use of VPNs. You can remind people that this concept is added to the glossary at the end of the slide and explain it based on that definition as follows:
  VPN, or Virtual Private Network, is a technology that creates a secure, encrypted connection over the internet, allowing users to browse privately and access geo-restricted content. Essentially, a VPN acts as a secure tunnel that encrypts your data and hides your IP address, protecting your privacy and security online.

Minute 30	**Facilitator Activity/Action**	**Strategy/Methodology**
	We move on to the second content topic of session 2	Introduction to the topic with an overview

Script/instructions

- Let's remember that we must always bear in mind that digital security is a complex field that is constantly evolving and that there is no such thing as 100% effective digital security, so the best approach is to improve our protection, and now we are going to address that topic.

Minute 31	**Facilitator Activity/Action**	**Strategy/Methodology**
	Begin the second content topic of session 2	Story about a descriptive visual

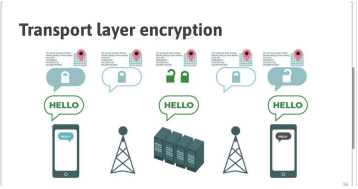
Script/instructions

- We already know that the risks are real, that those who want to attack us exploit vulnerabilities, and we remember the best practices. But when it comes to communications, we cannot emphasize enough that they must be encrypted. So the second topic we will cover in this session is that in order to protect our communications, we need to talk about encryption.
- *Read the slide*

Minute 34	**Activity/Action by the facilitator**	**Strategy/Methodology**
	Explain how encryption works in the transmission of information.	Narrative about a visual with infographics

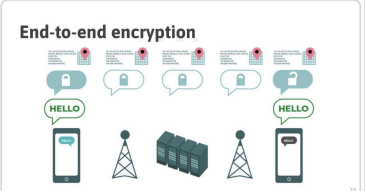
Script/instructions

- In this first graphic, you can see what the transmission of information would look like when I send a message to another person, both of us using cell phones. Anyone with access to the network can see the message we share. This is when we must remember what we saw in the first session: when transmitting a message over the internet, many companies participate in the activity. In other words, a third party does not even need to launch an attack to see the information I am sharing. When there is no encryption, anyone who is part of the transmission (the company that provides the internet service, the company that provides the messaging service, the company in charge of the servers, for example) will have access to the message.

Minute 37	**Facilitator's activity/action**	**Strategy/Methodology**
	Continue explaining the concept	Narrative about an infographic visual

Script/instructions

- In contrast, when we use a channel with encryption at the information transmission layer (at the information transport layer), the information cannot be seen while it is in transit. This would, for example, prevent the "man-in-the-middle attack" we talked about earlier, but other parties involved in the transfer, such as the company responsible for the private messaging application, will still be able to see the information, both for me and for the recipient. This is what is explained in the graph you are looking at.

Minute 40	**Activity/Action of the facilitator**	**Strategy/Methodology**
	Continue explaining the concept	Narrative about an infographic visual

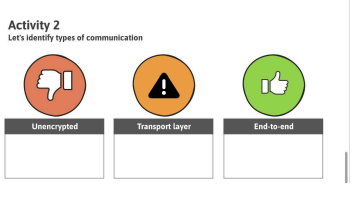
Script/instructions

- But using end-to-end encryption is even better. The difference with transport layer encryption is that the information is encrypted from the device on which I create it and is received encrypted by the recipient. This means that no intermediary company (such as internet and messaging service providers) has access to the information I share, which of course makes an external attack more difficult. It is worth noting that if someone who wants to access my information has access—physically or remotely—to the cell phone or computer I use, and that device does not have a password or is not encrypted, the information stored there, such as chats or backups, is easily accessible, but that is another issue worth considering.

Minute 45-55 BREAK	**Facilitator's activity/action**	**Strategy/Methodology**
	Rest	Stop for 10 minutes

Script/instructions

Interrupt the session to take a 10-minute break

Minute 55	**Facilitator's activity/action**	**Strategy/Methodology**
	Carry out the group activity for the second topic of session 2	Overview

Script/instructions

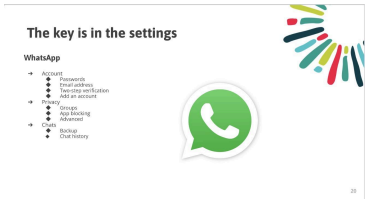
- It's time for the group activity. We are going to make a list of the forms of communication we use in our daily work in organizations and classify them into the following three groups.
  - Unencrypted (text messages, sites without https)
  - Transport layer (Telegram, Facebook Messenger, Twitter, Facebook, Instagram, websites with https, Zoom, Teams, Gmail, etc.)
  - End-to-end encryption (WhatsApp, Signal, secret Telegram messages, Teams for one-to-one calls)
- The main idea is to make us aware of the level of encryption our communications have, so that we can better analyze the risk we are taking.
- *The facilitator can help locate the tools and discuss any reflections that may arise with the course participants. Based on the questions you answered for this course, the most widely used networks in this group are Facebook, Twitter, and Instagram, while the most widely used private messaging tools are WhatsApp, followed by Facebook Messenger and Teams.*
- *Depending on the skills of the person facilitating the session, you may want to delve deeper into the type of encryption used by private messaging communication tools, where the industry standard is already end-to-end encryption. However, it is important for people to check that they are actually using encryption in the way the tools are configured.*
  - *End-to-end encryption in WhatsApp can be found here*
  - *End-to-end encryption in Messenger can be found here*
  - *End-to-end encryption in Teams can be found here*
  - *End-to-end encryption in Signal can be found here.*

Tips on other tools are in the final slides, which offer more resources.

Minute 60	**Facilitator activity/action**	**Strategy/Methodology**
	Introduction to the third content topic of session 2	Overview

Script/instructions

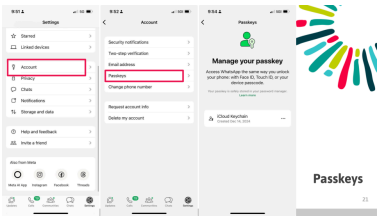
- We now move on to the last topic of this session. We know that using these tools has many benefits, so the goal is not to stop using them, but rather to find a balance between the benefits they offer and the risks, threats, and vulnerabilities they represent. Once again, this balance is the key to proper digital security management from the perspective of risk analysis on the one hand and the adoption of best practices on the other.
- We will do this by showing how to strengthen the security and privacy of a tool in its settings. The tool we are going to look at is the one that appeared to be most used by you in the survey: WhatsApp.

Minute 61	**Activity/Action by the facilitator**	**Strategy/Methodology**
	Present the third content topic of session 2, which is a practical exercise in itself.	Narrative with descriptive visuals.

Script/instructions

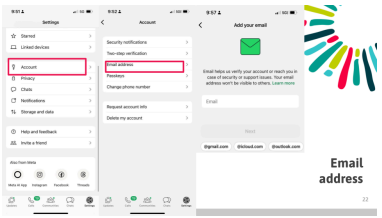
- WhatsApp was reported as the tool most used by people in this group, so we are going to do a practical exercise to improve its security by reviewing the tool's settings. We are going to use this application as an example to see the importance of configuring tools to improve our security and privacy. The exercise will focus on some of the elements that can be adjusted in WhatsApp.
- *Read the slide*
- However, the idea is that this serves as a starting point for you to explore other WhatsApp settings and, using this as an example, explore the other applications you normally use.

SUGGESTION. Depending on the skill of the person facilitating the exercise, you can take advantage of it to create a dynamic and prioritize the settings, making sure to explain the ones that generate the most interest, because it is difficult to predict how long it will take to make these adjustments, and you may only get through half of the list.

Minute 63	**Activity/Action by the facilitator**	**Strategy/Methodology**
	Develop the third content topic of session 2, which is a practical exercise in itself.	Story about a descriptive visual

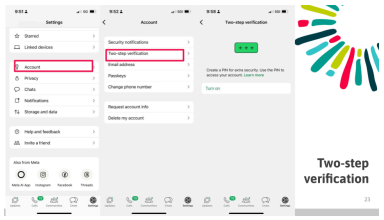
Script/instructions

- Let's start by requiring a password to access the application.
- On the slide, you can see the steps we will take to add a password to WhatsApp, a good password: one that has upper and lower case letters, at least one number, and a special character.
- *To do this, follow the graphic instructions on the slide. It is recommended that the person facilitating the exercise do it beforehand to be more confident in their presentation.*

Minute 68	**Activity/Action by the facilitator**	**Strategy/Methodology**
	Develop the third content topic of session 2, which is a practical exercise in itself.	Narrative about a descriptive visual.

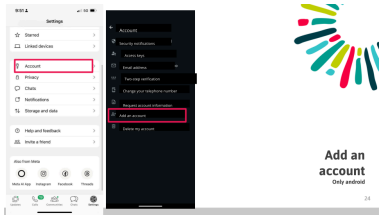
Script/instructions

- Let's now add an email account to communicate with WhatsApp
- On the slide, you can see the steps we will take to start adding an email address that will better protect your account. This allows you to verify it (even if you are traveling and cannot receive SMS messages) and creates an alternate channel of communication with WhatsApp to notify you of security issues.
- *Read the slide*
- *To do this, follow the graphic instructions on the slide. It is recommended that the person facilitating the exercise do it beforehand to be more confident in their presentation*

Minute 73	**Facilitator's activity/action**	**Strategy/Methodology**
	Present the third content topic of session 2, which is a practical exercise in itself.	Narrative about a descriptive visual.

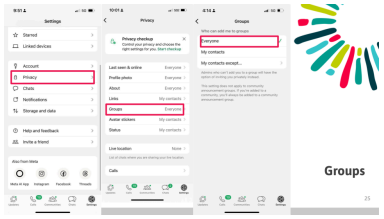
Script/instructions

- The slide shows the steps we can take to create a "two-step verification" or 2FV, which, as we have said on other occasions, is a very important element for the digital security of the applications we use.
- *Read the slide*
- *To do this, follow the graphic instructions on the slide. It is recommended that the facilitator do the exercise beforehand to be more confident in their presentation.*

Minute 78	**Activity/Action by the facilitator**	**Strategy/Methodology**
	Present the third topic of session 2, which is a practical exercise in itself.	Narrative about a descriptive visual.

Script/instructions

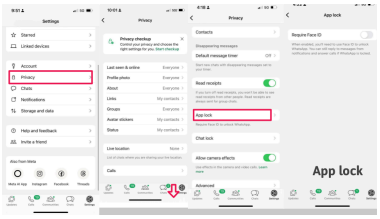
- A good security practice is to separate personal accounts from work accounts. If you want to do this, you can have two accounts set up on your cell phone. Please note that this does not apply to iPhones, but it does apply to Android phones.
- *Read the slide*
- *To do this, follow the graphic instructions on the slide. It is recommended that the facilitator do the exercise beforehand to be more confident in their presentation. Invite participants to explore the settings further; they may find other features they want to change.*

Minute 82	**Facilitator activity/action**	**Strategy/Methodology**
	Present the third content topic of session 2, which is a practical exercise in itself.	Narrative about a descriptive visual

Script/instructions

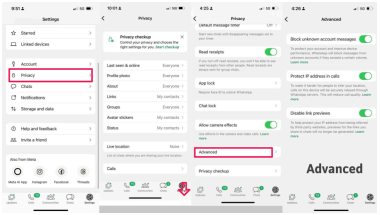
- There are also some things we can do to improve WhatsApp privacy
- *Read the slide*
- The slide shows the types of changes we can make. You can take some time to review the settings and decide what best suits your practices, but we will go through at least three specific elements, starting with

groups. Those who are in many groups should know that they can limit who can add them to a group. In any case, if someone who cannot add them to a group wants to do so, they can invite them, but they will have to send a link.

Minute 86	**Facilitator's activity/action**	**Strategy/Methodology**
	Introduce the third content topic of session 2, which is a practical exercise in itself	Story about a descriptive visual

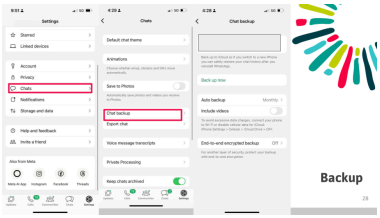
Script/instructions

- Another element that we can adjust in privacy is to choose to block the application, so that it requires our intervention to activate.
- *Read the slide*
- *To do this, follow the graphic instructions on the slide. It is recommended that the facilitator do the exercise beforehand to feel more confident in their presentation.*

Minute 90	**Facilitator activity/action**	**Strategy/Methodology**
	Present the third content topic of session 2, which is a practical exercise in itself.	Narrative about a descriptive visual.

Script/instructions

- There are other more advanced privacy settings that can be adjusted. I suggest you enable IP address protection and disable link previews (also to protect your IP address), as this reduces the application's ability to locate and profile us. Keep in mind that this is primarily a matter of preference; know that you can do it, but you don't have to.
- *Read the slide*
- *To do this, follow the graphic instructions on the slide. It is recommended that the facilitator do the exercise beforehand to be more confident in their presentation.*

Minute 94	**Facilitator activity/action**	**Strategy/Methodology**
	Present the third content topic of session 2, which is a practical exercise in itself.	Narrative about a descriptive visual.

Script/instructions

- Finally, let's talk about the adjustments we can make to the chats or conversations themselves. Essentially, it's about defining how we want to make backups. Now, there are some people who protect themselves by not having backups and treating their conversations as something ephemeral; in fact, they set their chats to disappear every so often. This depends on what you want. Let's see how and where to decide if and how we want backups.
- *Read the slide*

Minute 100	**Facilitator activity/action**	**Strategy/Methodology**
	Additional resources Session 2	Additional resources that allow session participants to delve deeper

Script/instructions

- *Added to the glossary from the previous session VPN*