AFD AGENCE FRANÇAISE DE DÉVELOPPEMENT

Funded by the European Union

forus CONNECT SUPPORT INFLUENCE

INNOVUS

Security Digital and risk management

Session # 3

Best Practices

2025

1. General Information

1. Course/Workshop Name: Introduction to Digital Security for Non-Governmental Organizations (NGOs) & Human Rights Defenders (HRDs)
2. Duration: maximum 90 minutes
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; no prior knowledge is required, except for having completed the survey. For this session, the person facilitating the session should send slides 7, 8, 9, and 10 to the attendees' email addresses (this can be done by creating a ppt file with those two slides). The idea is that during the session, when it is time to carry out this activity, each person can have this file to hand and edit it, keeping their own version of the risk analysis and mitigation measures.

- Space setup: check the sound and image, and set up the projector screen. Ensure that the option to create groups is enabled and define how the groups will be formed (randomly or from a predetermined list).

- Support technologies: links, activities, and evaluation

- Preparation prior to the session (logistics, review of materials): Nothing, but don't forget to send slide 8.

- 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. Session 3 script (described slide by slide)

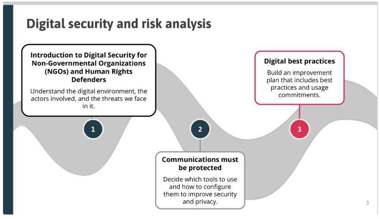
Minute 1. Security and and risk management Session #3: Best practices 2025 AFD Funded by the European Union forus INNOVUS 1	**Activity/Action tion of the facilitator** Welcome and present course objectives	**Strategy/Methodology** Story about a generic visual
Script/instructions		

- 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.

Minute 2.	**Activity/Action by the facilitator**	**Strategy/Methodology**
 Digital security and risk management Digital security? I don't know anything about that! Let's think about how to protect ourselves in digital media 2	Introduction to the topic	Story about a generic visual

Script/instructions

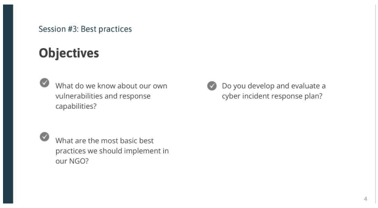
- We begin our third and final session on digital security with a focus on risk analysis. We hope that by this point in the course, you will be able to say that you have acquired basic knowledge of the topic and that you have an understanding of, and especially new tools for, how to protect yourself when you inhabit and use digital media.
- We reiterate that it is because people improve their knowledge of digital security that they can use technology safely, privately, and with confidence. It is important to reiterate once again that a balanced view of digital security puts people at the center.
- Let 's get started!

Minute 3	**Facilitator activity/action**	**Strategy/Methodology**
 Digital security and risk analysis **Introduction to Digital Security for Non-Governmental Organizations (NGOs) and Human Rights Defenders** Understand the digital environment, the actors involved, and the threats we face in it. **Communications must be protected** Decide which tools to use and how to configure them to improve security and privacy. **Digital best practices** Build an improvement plan that includes best practices and usage commitments. 3	Introduction to the topic	Story about a descriptive visual

Script/instructions

- The course aims to provide participants with basic knowledge of digital security so that they can integrate it into the daily practices of NGOs and human rights organizations, thereby strengthening their resilience and sustainability.
- I would like to remind you that in this module, digital security is approached from a risk analysis perspective, and the specific idea of this third session is to think about digital security from the perspective of internal and external communications.
- In this third session, course participants will receive the tools they need to develop a basic plan for their organization that will enable them to improve everyday practices and, in turn, improve the digital security of those organizations.

Minute 4



Session #3: Best practices

Objectives

- What do we know about our own vulnerabilities and response capabilities?
- What are the most basic best practices we should implement in our NGO?
- Do you develop and evaluate a cyber incident response plan?

4

Activity/Action by the facilitator

Introduction to the topic

Strategy/Methodology

Story about a descriptive visual

Script/instructions

- During this third and final session, we will reflect on what we know about our own vulnerabilities and our ability to respond to those vulnerabilities. We will receive the basic elements for developing a cyber incident response plan, a task that your organizations will need to continue after this session.
- Finally, we will go through the 10 basic steps of a roadmap for improving digital security for your organizations.

Minute 6

Let's review the concepts of risk analysis

Facilitator activity/action

Introduction to the first topic of this session

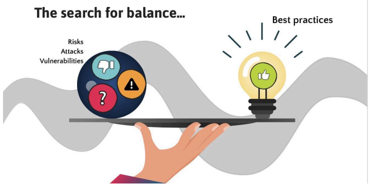
Strategy/Methodology

Story about a descriptive visual

Script/instructions

- The first thing we will do is review key concepts of digital security from a risk analysis perspective.

Minute 7



Activity/Action by the facilitator

Remember the balance in digital security issues

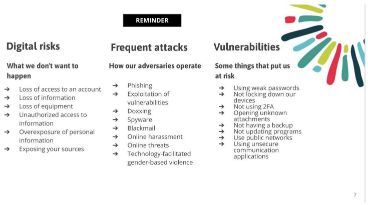
Strategy/Methodology

Informative visual narrative

Script/instructions

- To find the right balance in digital security, we must identify our risks, potential attacks, and vulnerabilities. This will allow us to establish best practices that can be implemented in organizations.

Minute 8



REMINDER

Digital risks

What we don't want to happen

- → Loss of access to an account
- → Loss of information
- → Loss of equipment
- → Unauthorized access to information
- → Overexposure of personal information
- → Exposing your sources

Frequent attacks

How our adversaries operate

- → Phishing
- → Exploitation of vulnerabilities
- → Doxxing
- → Spyware
- → Blackmail
- → Online harassment
- → Online threats
- → Technology-facilitated gender-based violence

Vulnerabilities

Some things that put us at risk

- → Using weak passwords
- → Not locking down our devices
- → Not using 2FA
- → Opening unknown attachments
- → Not having a backup
- → Not updating programs
- → Use public networks
- → Using unsecure communication applications

7

Activity/Action by the facilitator

Review the topics of risks, attacks, and vulnerabilities.

Strategy/Methodology

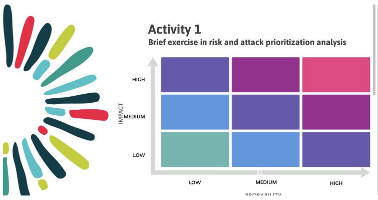
Narrative about a descriptive visual containing the text to be repeated.

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

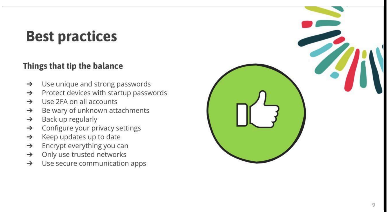
- *Read the slide.*
- We have talked at length about the risks, possible attacks, and the most common vulnerabilities you may encounter. Now we are going to divide into groups of 5 or 6 people for 10 minutes so that each group can share their experiences and determine which risks and attacks they have suffered most or fear most. This will be useful for activity 3 in this session. Each group should select the 4 risks and 4 attacks they consider most important in their activity.

PLATFORM REQUIREMENTS: The facilitator should set up the groups and time each group's activity.

Minute 20	**Facilitator's activity/action**	**Strategy/Methodology**
 **Activity 1** **Brief exercise in risk and attack prioritization analysis** HIGH MEDIUM LOW IMPACT LOW MEDIUM HIGH PROBABILITY	Activity	Story about a visual aid to carry out the activity.

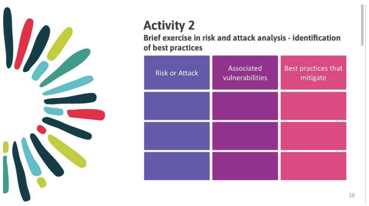
Script/instructions

- Considering the four risks and attacks/vulnerabilities that each group identified as most important in their activity, each person should now take the file they received before this session, which contains an editable version of the slide they are seeing on the screen.
- The idea is that you now reflect on how likely it is that each of the four attacks or risks you identified will occur and what the impact would be on your work. For example, if you identified that information loss is a real risk in your organization, define the probability of it occurring (high, medium, or low) and its impact on the organization (high, medium, or low). As you fill in the table, you will have to decide this for the others on your list, as in the end there should only be one attack or risk per table. This is a way of prioritizing so that the table ends up as a heat map. This will allow you to define the priority for addressing the main risks and attacks.
- If you like, keep in mind that in the activity you did with your group, you chose the eight most important risks and attacks in your organizations. The table offers nine spaces, so now you have the opportunity to make adjustments for your own organization and add a ninth, but it is not necessary. Do as much as you can; you don't have to do a perfect exercise. Think of this activity as a first reflection that you can continue working on after this course.
- I will give you five minutes to do the exercise. Let's begin.
- *The facilitator will give you five minutes to complete the exercise.*
- Okay, the five minutes are up. What you can see in the table that each person completed is a first version of your organization's risk analysis. In red, you see the risk or vulnerability that is most urgent for your organization to address, followed by those in burgundy, then purple, blue, and finally green. This preliminary exercise will help you discuss within your organizations and agree on the final table you will work with.
- *Open the microphone for a couple of minutes to hear people's opinions about the exercise.*

Minute 30	**Facilitator's activity/action**	**Strategy/Methodology**
 **Best practices** **Things that tip the balance** → Use unique and strong passwords → Protect devices with startup passwords → Use 2FA on all accounts → Be wary of unknown attachments → Back up regularly → Configure your privacy settings → Keep updates up to date → Encrypt everything you can → Only use trusted networks → Use secure communication apps 	Review the topics of good practices.	Narrative about a descriptive visual that recalls information already provided.

Script/instructions

- As we saw in the last session, the most frequent risks for non-governmental organizations and human rights organizations occur because there are also frequent attacks that exploit a series of vulnerabilities that are present in the digital environment. The way to mitigate this is by adopting good practices. Remember this. Use this slide to follow the exercise.

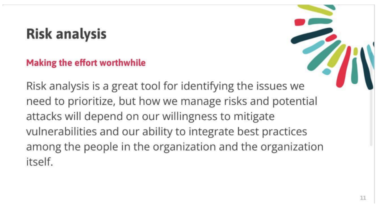
<table>
<tr>
<td>Minute 32

<b>Activity 2</b>
<b>Brief exercise in risk and attack analysis - identification of best practices</b>
<table>
<tr><th>Risk or Attack</th><th>Associated vulnerabilities</th><th>Best practices that mitigate</th></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
</table>
10</td>
<td><b>Facilitator's activity/action</b>
Activity</td>
<td><b>Strategy/Methodology</b>
Narrative about a visual aid to carry out the activity.</td>
</tr>
</table>

Script/instructions

- Considering the risks and vulnerabilities identified by each group as most important to their activity, we will now do a group exercise.
- The idea is for you to reflect on how likely each of the four attacks or risks you identified is to occur and what the impact would be on your work. For example, if you identified information loss as a real risk in your organization, define the probability of it occurring (high, medium, or low) and its impact on the organization (high, medium, or low). As you fill in the table, you will have to decide this for the others on your list, as in the end there should only be one attack or risk per table. This is a way of prioritizing so that the table ends up as a heat map. This will allow you to define the priority for addressing the main risks and attacks.
- If you like, keep in mind that in the activity you did with your group, you chose the eight most important risks and attacks in your organizations. The table offers nine spaces, so now you have the opportunity to make adjustments for your own organization and add a ninth, but it is not necessary. Do as much as you can; you don't have to do a perfect exercise. Think of this activity as a first reflection that you can continue working on after this course.
- I will give you five minutes to do the exercise. Let's begin.
- *The facilitator will give you five minutes to do the exercise.*
- Well, the five minutes are up. What you can see in the table that each person has completed is a first version of your organization's risk analysis. In red, you see the risk or vulnerability that is the highest priority for your organization to address, followed by those in burgundy, then purple, blue, and finally green. This preliminary exercise will help you discuss within your organizations and agree on the final table you will work with.
- *Open the microphone for a couple of minutes to hear people's opinions about the exercise.*

SUGGESTION: The facilitator should be enthusiastic in this explanation. After a module that is a bit discouraging, the feeling should remain that it is possible to do something.

Minute 42

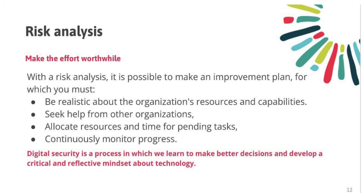


Risk analysis

Making the effort worthwhile

Risk analysis is a great tool for identifying the issues we need to prioritize, but how we manage risks and potential attacks will depend on our willingness to mitigate vulnerabilities and our ability to integrate best practices among the people in the organization and the organization itself.

11



Risk analysis

Make the effort worthwhile

With a risk analysis, it is possible to make an improvement plan, for which you must:

- Be realistic about the organization's resources and capabilities.
- Seek help from other organizations,
- Allocate resources and time for pending tasks,
- Continuously monitor progress.

Digital security is a process in which we learn to make better decisions and develop a critical and reflective mindset about technology.

12

Facilitator activity/action

We move on to the second topic of session 3

Strategy/Methodology

Introduction to the topic with an overview

Script/instructions

- To conclude this point, let's make some final reflections
- *Read the conclusion slides*

Minutes 45-55
BREAK

Activity/Action by the facilitator

Rest

Strategy/Methodology

Stop for 10 minutes

Script/instructions

Minute 55

A possible path

13

Activity/Action by the facilitator

We move on to the second topic

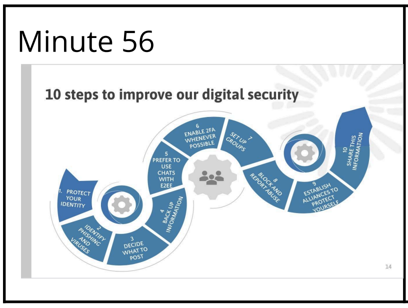
Strategy/Methodology

Story about a descriptive visual

Script/instructions

- In addition to the fact that risk analysis provides your organization with a roadmap for addressing the risks and attacks that have been prioritized, we would also like to provide you with a roadmap that can be useful to any non-governmental organization and those who defend human rights. Let's take a look.

Minute 56



10 steps to improve our digital security

1. PROTECT YOUR IDENTITY
2. IDENTIFY PHISHING AND VIRUSES
3. DECIDE WHAT TO POST
4. BACK UP INFORMATION
5. PREFER TO USE CHATS WITH E2EE
6. ENABLE 2FA WHENEVER POSSIBLE
7. SET UP GROUPS
8. BLOCK AND REPORT ABUSE
9. ESTABLISH ALLIANCES TO PROTECT YOURSELF
10. SHARE THIS INFORMATION

14

Activity/Action by the facilitator

Explain the roadmap for basic improvements in organizations' digital security.

Strategy/Methodology

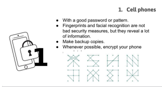
Narrative about an informative visual

Script/instructions

- Based on what we know about the most common risks, attacks, and vulnerabilities among NGOs and human rights organizations, we know that the best way to improve digital security would be an improvement plan for our organization that would allow us to reflect on each step and make decisions. Sometimes these are internal changes (which the following slides can help with), other times it is developing policies, and other times it may mean identifying who can help us.
- *The facilitator will read each of the 10 steps.*

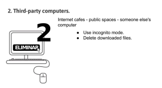
Minute 59

10 basic recommendations



1. Cell phones

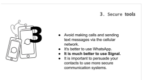
- With a good password or pattern.
- Fingerprints and facial recognition are not bad security measures, but they reveal a lot of information.
- Make backup copies.
- Whenever possible, encrypt your phone



2. Third-party computers.

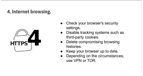
Internet cafes - public spaces - someone else's computer

- Use incognito mode.
- Delete downloaded files.



3. Secure tools

- Avoid making calls and sending text messages via the cellular network.
- It's better to use WhatsApp.
- **It is much better to use Signal.**
- It is important to persuade your contacts to use more secure communication systems.



4. Internet browsing.

- Check your browser's security settings.
- Disable tracking systems such as third-party cookies.
- Delete compromising browsing histories.
- Keep your browser up to date.
- Depending on the circumstances, use VPN or TOR.

Activity/Action by the facilitator

Continue explaining the concept.

Strategy/Methodology

Story about an infographic visual

Script/instructions

- Finally, let's take a moment to look at 10 important recommendations for improving our digital security. These are changes we can make in our everyday use of technology and that we should encourage throughout the organization. Part of the process of following the path we saw earlier is to reflect on which of these recommendations we should integrate into each step. You will need to do this in your organizations later on. Let's begin
- *(Going through the slides one by one, the person facilitating the session will pause at each one).*
- Recommendation 1. The passwords we use on our devices are important and should not be underestimated, as they are the first element of our digital security. That is why we must pay attention to the passwords that protect them. Here are some ideas that you can implement on your cell phones to address risks, prevent attacks, and mitigate our vulnerabilities*. Read the slide.*
- Recommendation 2. The survey found that several of the participants in this course use internet cafes, public spaces (remember the case we saw last session about public Wi-Fi in airports), or someone else's computer to connect to the network. The tips and guidelines on how to protect ourselves in these circumstances are especially important for organizations where this happens. *Read the slide*
- Recommendation 3. During the course, we talked about the importance of encrypted communications, which means that we need to be very conscious of using secure tools in our daily lives. We suggest that you adopt the following practices, which will help you to always think about which tools are secure and preferable. *Read the slide*
- Recommendation 4. Regular use of the internet in our organizations and the information we reveal about people and organizations through browsing should lead us to better evaluate the tools we use for browsing and even think about how we configure them. Remember the exercise we did to configure WhatsApp more securely. You can search for tutorials for your browsers and also do the exercise with these tools. In any case, it is also important to remember that sometimes security measures slow down browsing and therefore, in conditions of poor connectivity, there are precautions that are best not to take. *Read the slide*

Minute 68

5. Backups.

- Backup, backup, backup
- Encrypt, encrypt, encrypt.

Google to Encrypt Android Cloud Backups With Your Lock Screen Password

October 15, 2018 Swati Khandelwal

In an effort to secure users' data while maintaining privacy, Google has announced a new security measure for Android Backup Service that now encrypts all your backup data stored on its cloud servers in a way that even the company can't read it.

Facilitator Activity/Action

Continue explaining the recommendations for the route

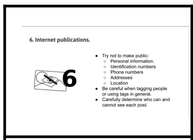
Strategy/Methodology

Narrative about an infographic visual

Script/instructions

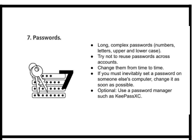
- Recommendation 5. Considering that there is no such thing as 100% digital security, one way to deal with the risks is to mitigate their effects. Making backup copies is an effective way to mitigate the risks of information loss. However, the copies must be encrypted. That is why it is important to analyze the tool we use, configure it, and understand how our information is protected. It is worth remembering that some people intentionally choose to have only ephemeral communications and make sure to delete all their messages quickly as a form of protection. This is also valid and is usually the result of deep reflection. *Recommendation 5 Read the slides.*
- *(The next slide elaborates further on this recommendation.)* It is worth pausing for a moment on this recommendation, as there are different ways to make backup copies. The important thing is to review which is most functional for each organization. You can use your own devices (USB or hard drives) or third-party cloud services such as Google Drive or iCloud. In any case, sensitive information must be encrypted. You can use VeraCrypt for this.

Minute 75



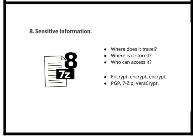
6. Internet publications.

- Try not to make public:
  - Personal information.
  - Identification numbers
  - Phone numbers
  - Addresses
  - Location
- Be careful when tagging people or using tags in general.
- Carefully determine who can and cannot see each post.



7. Passwords.

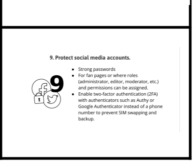
- Long, complex passwords (numbers, letters, upper and lower case).
- Try not to reuse passwords across accounts.
- Change them from time to time.
- If you must inevitably set a password on someone else's computer, change it as soon as possible.
- Optional: Use a password manager such as KeePassXC.



8. Sensitive information.

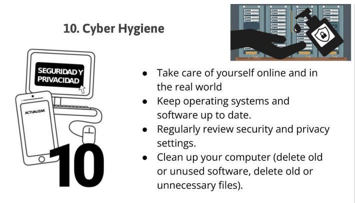
- Where does it travel?
- Where is it stored?
- Who can access it?

- Encrypt, encrypt, encrypt.
- PGP, 7-Zip, VeraCrypt.



9. Protect social media accounts.

- Strong passwords
- For fan pages or where roles (administrator, editor, moderator, etc.) and permissions can be assigned.
- Enable two-factor authentication (2FA) with authenticators such as Authy or Google Authenticator instead of a phone number to prevent SIM swapping and backup.



10. Cyber Hygiene

- Take care of yourself online and in the real world
- Keep operating systems and software up to date.
- Regularly review security and privacy settings.
- Clean up your computer (delete old or unused software, delete old or unnecessary files).

Facilitator Activity/Action

Continue explaining the recommendations for the route.

Strategy/Methodology

Narrative about an infographic visual

Script/instructions

- Recommendation 6. We must be careful with the information we publish on the internet because it reveals a lot about people, their personal and professional circles, and also about the organizations they work for or represent. We suggest a series of reflections so that decisions about the organization's information are intentional: *Read the slide*
- Recommendation 7. Let's talk about passwords again, this time for the tools we use. In the surveys, several people said they reuse passwords and several said they keep their browsers open all the time. At this point in the course, we are surely clear that good password practices are perhaps the most basic element of our digital security. *Read the slide*
- Recommendation 8. One of the important tasks that should be left to those who participated in the course is to think about the sensitive information they handle in the organization. This depends greatly on the type of organization and the data they hold. If it is an organization that works on issues of violence against women, it must define how the data they have is handled and how and with whom they share it. Something similar happens with organizations that work with migrants, for example. However, every organization must analyze

the information it has and define its degree of sensitivity. For example, you have a lot of data on the people who work for you, which, if leaked or disclosed by you, could be used for fraud, blackmail, or even abuse and some forms of gender-based or other violence. That is why we suggest that you ask yourselves some questions and reflect on the sensitive information you have. This will help you understand the importance of taking measures to protect it. Failure to do so may violate the privacy of others and may also put the organization itself at risk: *Read the slides.*

- Recommendation 9. In the survey, we established that many organizations use social media to publish information. Therefore, it is advisable for those participating in this course to analyze how they use these networks and understand that there are measures that can be taken to make this activity safe: *Read the slide*.
- Recommendation 10. Finally, while making backups is a good practice, implementing "cyber hygiene" measures, which include deleting information from time to time, is also an important element of your organizations' digital security: *Read the slide.*

We have reached the end of our module on digital security. Perhaps one final message we can leave you with is that digital security is highly contextual. The risks we face, the possible attacks, several of the vulnerabilities we may be subject to, as well as the measures we can take to mitigate and avoid these circumstances, depend largely on where we live or work, the people around us, the conditions of our connectivity, the equipment we have access to, and a long list of other factors. Therefore, it is important that we understand that: "there is no such thing as complete security," "there are no one-size-fits-all solutions," and "our personal security depends on that of the group." Thank you for joining us on this journey.