Security
and
and risk management

Session #3: Best practices

2025

AFD AGENCE FRANÇAISE DE DÉVELOPPEMENT

Funded by the European Union

forus CONNECT SUPPORT INFLUENCE

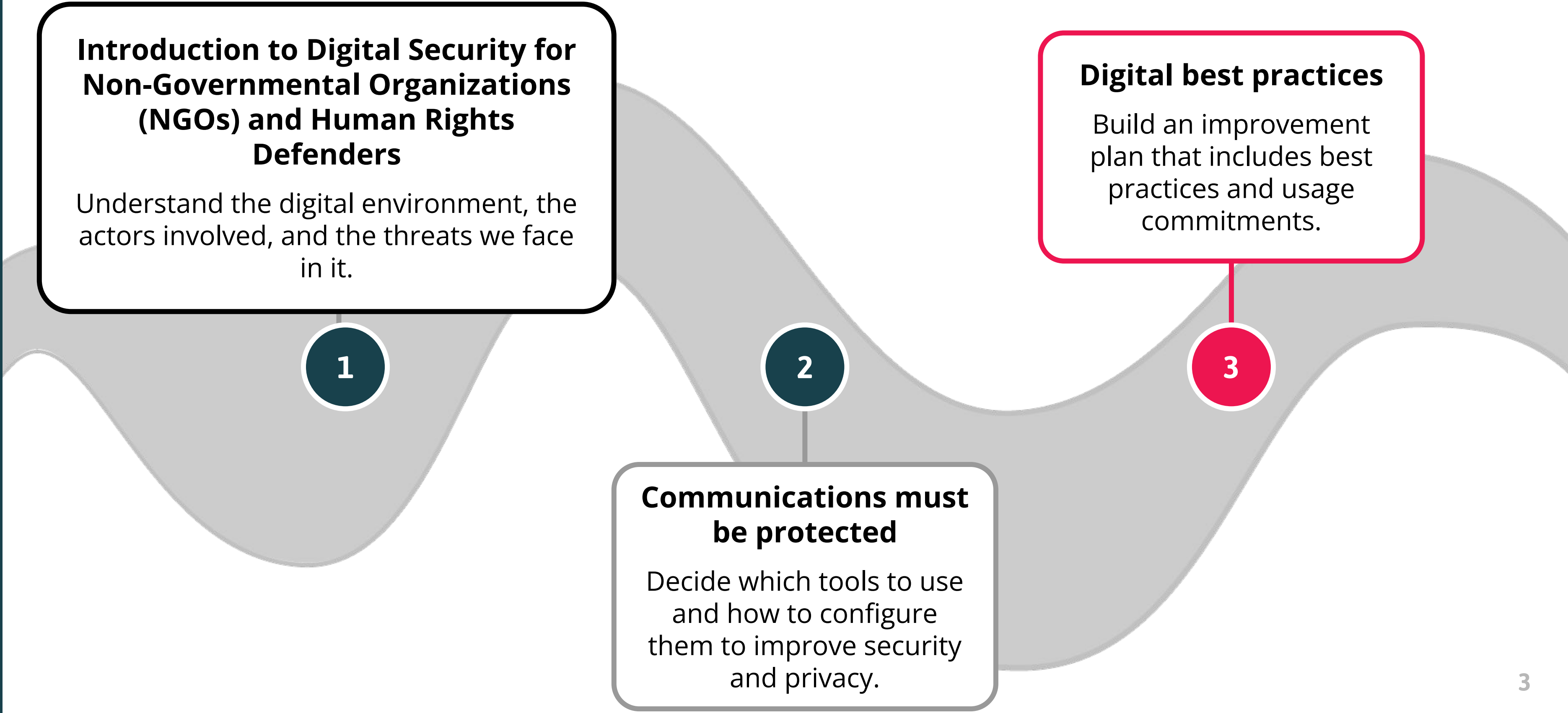
INNOVUS

Digital security?
I don't know anything about that!

Let's think about how to protect ourselves

in digital media

Digital security and risk analysis



1

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.

2

Communications must be protected

Decide which tools to use and how to configure them to improve security and privacy.

3

Digital best practices

Build an improvement plan that includes best practices and usage commitments.

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?

Let's review the concepts of risk analysis

The search for balance...

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

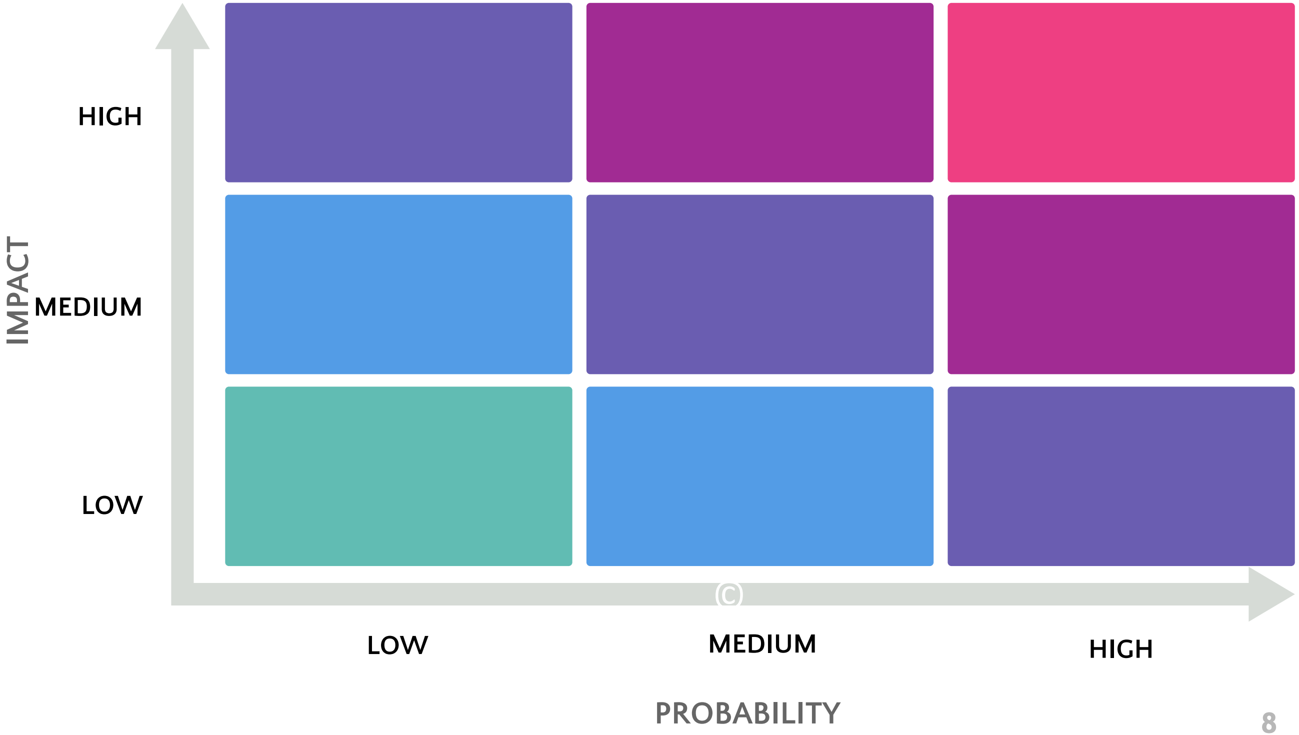
Vulnerabilities

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

Activity 1

Brief exercise in risk and attack prioritization analysis



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

Activity 2

Brief exercise in risk and attack analysis - identification of best practices

Risk or Attack	Associated vulnerabilities	Best practices that mitigate

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.

Risk analysis

Make the effort worthwhile

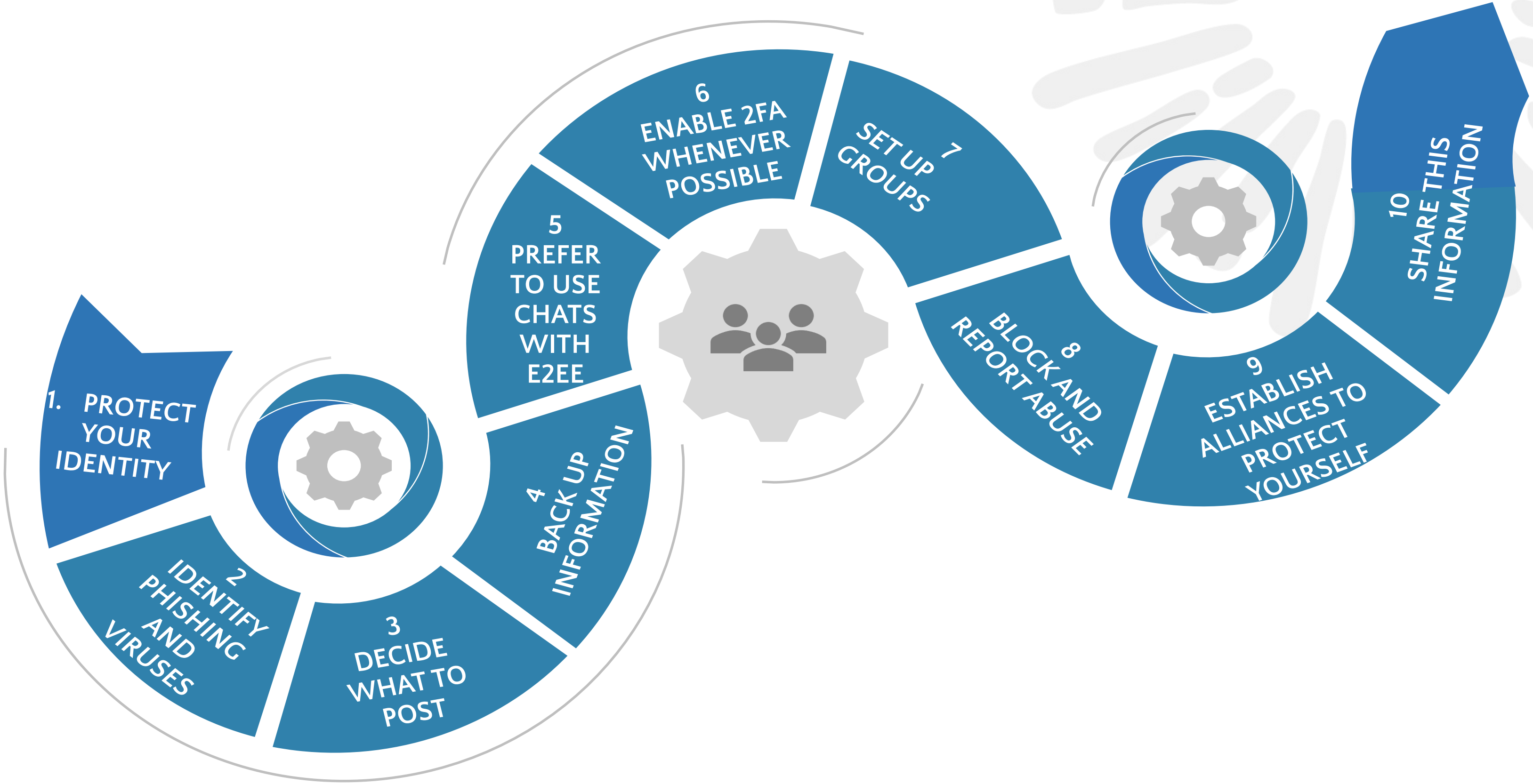
With a risk analysis, it is possible to make an improvement plan, for which you must:

- 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.

A possible path

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

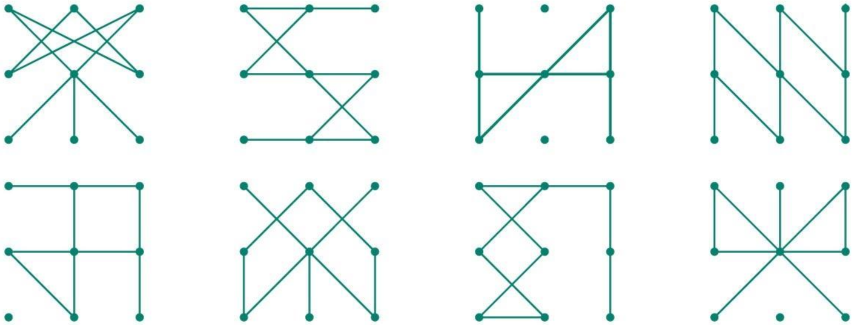
9 ESTABLISH ALLIANCES TO PROTECT YOURSELF

10 SHARE THIS INFORMATION

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**

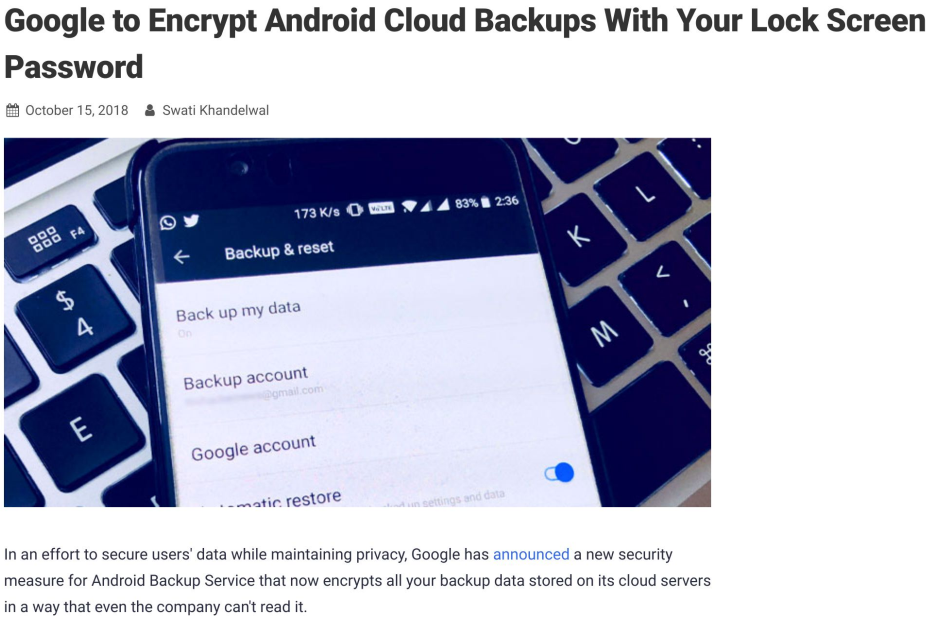
- Avoid making calls and sending text messages via the cellular network.
- It's better to use WhatsApp.
- **It is much better to use Signal.**
- It is important to persuade your contacts to use more secure communication systems.

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.

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.

Examples of ways to make backup copies.

VeraCrypt

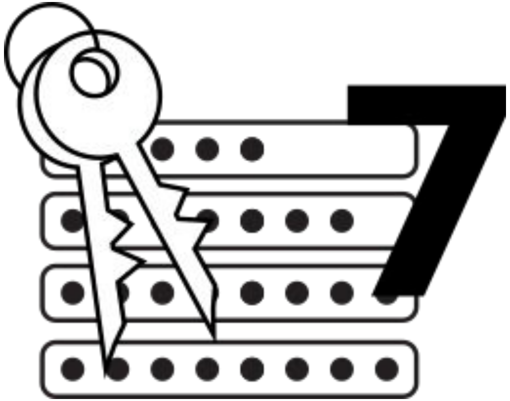
Google Drive

iCloud

6. Internet publications.

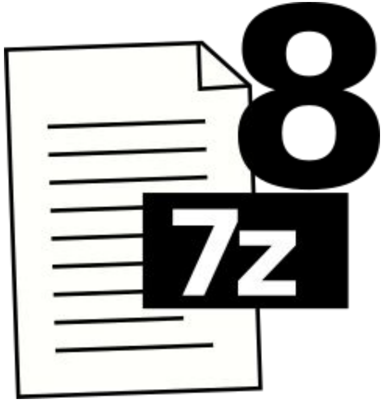
- Try not to make public:
  - Personal information.
  - Identification numbers
  - Phone numbers
  - Addresses
  - Location
- Be careful when tagging people or using tags in general.
- Carefully determine who can and cannot see each post.

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.



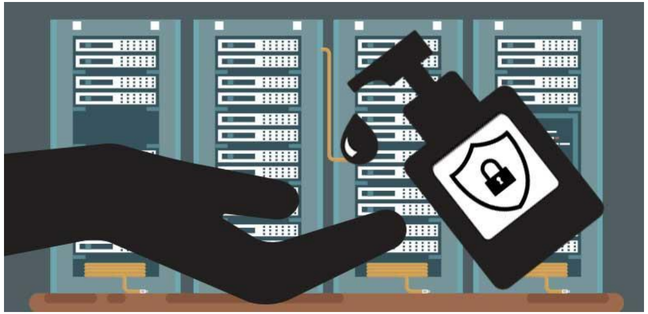
- Where does it travel?
- Where is it stored?
- Who can access it?

- 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).

Thank you!

INNOVUS

www.innovusconsulting.co

Session facilitators: Catalina Valenzuela, Paula Quiñones, and Camilo Forero

Module creator: Carolina Botero