Security and and risk management

Session #1: Introduction to digital security for non-governmental organizations (NGOs) & human rights defenders

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

Introduction to digital security for non-governmental organizations (NGOs) and human rights defenders

Understanding the digital environment, the actors involved, and the threats we face in it.

1

2

Take care with communications

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 #1: Introduction to digital security for non-governmental organizations (NGOs) and human rights defenders

Objectives

- Identify how the internet works and the role of intermediary companies.
- Identify the digital tools we use most.
- Identify the risks, threats, vulnerabilities, and capabilities that NGOs and human rights defenders face when using such tools.

Digital security is a collaborative effort and a shared responsibility

1. How the internet works

How many companies are needed for the mail to work?

Internet intermediaries

- The internet was originally conceived as a **decentralized**, **open**, and **neutral** space.
- The Internet is now a **space dominated** by a few large technology companies (Alphabet, Amazon, Meta, Apple, Microsoft) that **define the digital lives** of billions of people.
- It is necessary **to understand how the internet works** in order to **agree on uses** and **practices** from the **contexts** of our organizations and their **needs.**

The internet is a space that we can use for our activism.

Activity 1

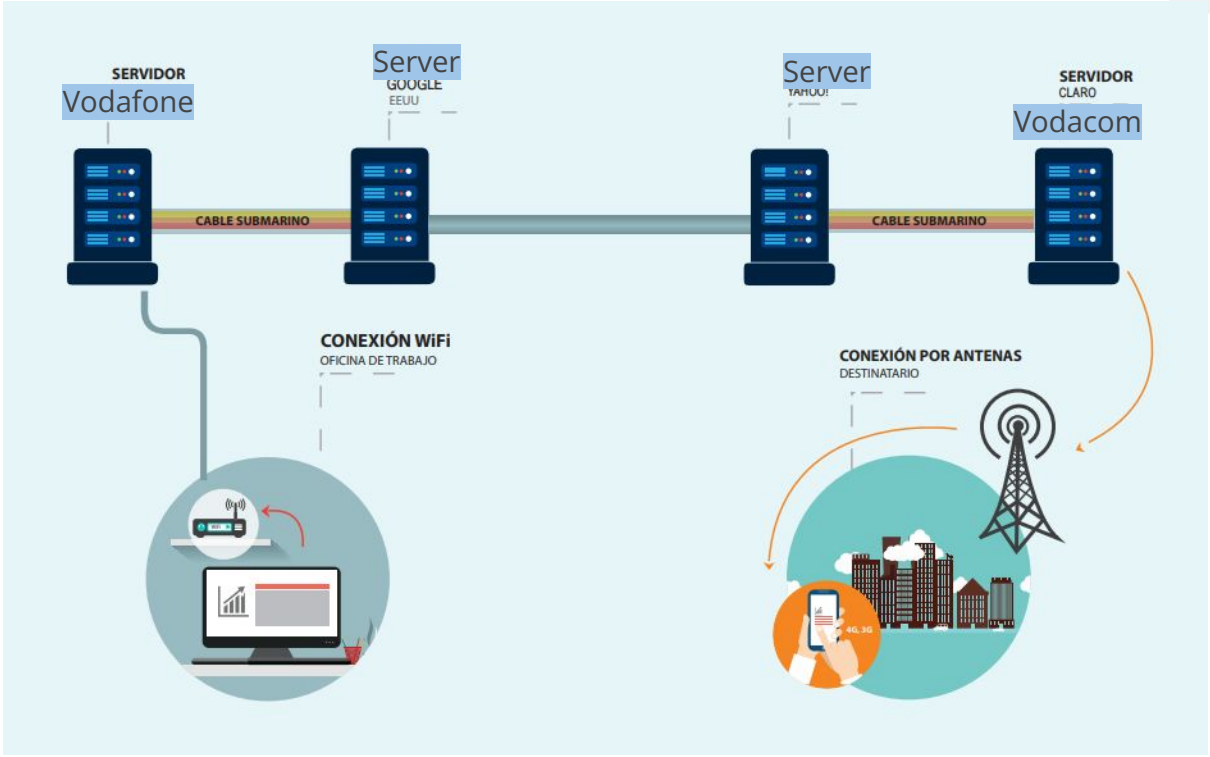
Let's send an email

Let's imagine that Ana sends an email to Juan from her laptop connected via WiFi to Vodafone or the local internet carrier provider. She uses a Google email account. Juan uses a Yahoo! account and reads the email on his cell phone, which is connected to a cell phone such as Vodafone prepaid plan.

Which intermediary companies do we recognize?

How do they communicate with each other?

What devices are involved?


SERVIDOR
Vodafone
Server
GOOGLE
EEUU
Server
YAHOO!
SERVIDOR
CLARO
Vodacom
CABLE SUBMARINO
CABLE SUBMARINO
CONEXIÓN WiFi
OFICINA DE TRABAJO
CONEXIÓN POR ANTENAS
DESTINATARIO
4G, 3G

How many companies are needed for the mail to function?

Internet intermediary companies

- There are different types of intermediaries
  - Access providers
  - Hardware manufacturers
  - Domain name providers
  - Hosting providers
  - Search engines
  - Content creators
  - Social networks
  - E-commerce
  - Web analytics and surveillance providers
- Multiple companies are involved in every activity we carry out on the internet
- Our security and that of our information depends on these companies and on our decisions

Let's reflect on our relationship with these companies

2. Inventory

What applications and services do we use on a daily basis?

Our digital ecosystem

- The digital **experience** is unique and depends on our **contexts**, **needs**, and usage **practices**.
- It is possible to talk about degrees of **digital appropriation**
  - Non-users
  - Basic: Communication and entertainment
  - Intermediate: Education and participation
  - Advanced: Transactions and sophisticated uses (holding online events, researching, downloading and configuring programs, making transfers to third parties)
- For basic and intermediate uses, it is possible **to define trends** and propose **best practices** for use. For advanced uses, it is good to think about **protocols**.

Activity 2

Let's make a list of the main applications we use at work.

Communications (int)

Productivity (internal)

Participation (ext)

What apps and services do we use on a daily basis?

Our digital ecosystem

- Practicing safe habits requires talking openly about how we use technology, recognizing what we are doing well, what could be improved, and changing some habits.
- Digital security is a process in which we learn to make better decisions and develop a critical and reflective mindset about technology.
- In an organization, security depends on everyone.
- The best thing to do is to be prepared for potential problems and learn from incidents.

We can create a culture of digital security in which everyone plays a part.

3. Risk analysis

The search for balance...

Best practices

Risks
Attacks
Vulnerabilities

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
- ➔ Not updating the computer's operating system

Which of these risks have you already faced? How did you handle them? What were the consequences?

Which of these risks do we fear the most? And why?

Frequent attacks

How our adversaries operate

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

Which of these attacks have we already faced? How did you handle them? What were the consequences?

Which of these attacks do we fear the most? And why?

Vulnerabilities

Some things that put us at risk

- ➔ Using weak passwords
- ➔ Not locking devices
- ➔ Not using 2FA
- ➔ Opening unknown attachments
- ➔ Not having a backup
- ➔ Not updating programs
- ➔ Use public networks
- ➔ Using insecure communication applications

Which of these vulnerabilities do we recognize?

Are there any that cannot be changed? If so, why?

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

Are there any best practices from this list that you would like to implement?

Any that you would like to add?

Glossary

Risk analysis: Risk analysis, also known as risk assessment or PHA (Process Hazards Analysis), is the study of the causes of potential threats and probable undesirable events and the damage and consequences they may cause.

Internet intermediary: An internet intermediary refers to a company that facilitates the use of the internet. These companies include internet service providers (ISPs), search engines, and social media platforms.

Phishing: This is a computer term that refers to a set of techniques that seek to deceive a victim by gaining their trust by posing as a trusted person, company, or service (trusted third-party impersonation) in order to manipulate them into performing actions they should not perform (e.g., revealing confidential information or clicking on a link).

Exploitation of vulnerabilities. Vulnerabilities are flaws in computer systems that can be exploited by an attacker to perform unauthorized actions that can compromise the security of the information contained in the systems or the functioning of those systems themselves.

Doxxing: The terms doxing and doxxing describe the act of intentionally and publicly revealing personal information about an individual or organization, usually via the internet.

Spyware: Spyware is malware that collects information from a computer and then transmits this information to an external entity without the knowledge or consent of the computer owner.

Blackmail: Blackmail (from the French chantage) is the threat of public defamation or similar harm to obtain some financial or material gain from someone or to force them to act in a certain way. Blackmail or extortion is a crime in the legal systems of many countries.

Online harassment; Cyberbullying, also known as virtual harassment, is the use of digital media to harass or bully one or more people through personal attacks, disclosure of personal or false information, among other means. Acts of cyber aggression have specific characteristics, which are the anonymity of the aggressor, their speed, and their reach.

Online threats: also known as cyber threats, these are any malicious acts that seek to compromise the security of computer systems, networks, or devices in order to gain unauthorized access, steal data, cause damage, or disrupt operations.

Digital gender-based violence, also known as technology-facilitated gender-based violence, refers to any act of violence that occurs online and is directed at individuals on the basis of gender. This violence manifests itself through various digital media, such as social networks, cell phones, and internet platforms, and can include harassment, threats, and the dissemination of intimate content without consent, among other things.

Thank you!

www.innovusconsulting.co

Session facilitators:
Catalina Valenzuela,
Paula Quiñones
Camilo Forero

Module creator: Carolina Botero