Funded by the European Union

Security Digital and risk management

Session #1

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

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 necessary, except for having completed the survey. 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): None.
- 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 1 script (described slide by slide)

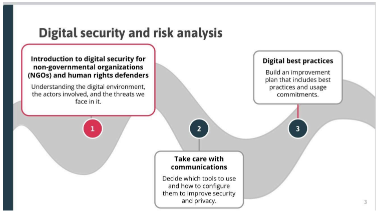
<table>
<tr>
<td>Minute 1.
 Security
and
and risk management
Session #2: Communications must be handled with care
2025

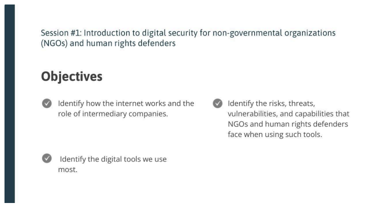
AFD
Funded by the European Union
forus
INNOVUS
1

</td>
<td><b>Activity/Facilitator Action</b>
Welcome and present course objectives</td>
<td><b>Strategy/Methodology</b>
Story about a generic visual</td>
</tr>
<tr>
<td colspan="3"><b>Script/instructions</b>
1. Welcome to the course Introduction to Digital Security for NGOs & HRDs
2. Facilitator's name: xxxxx
3. No prior knowledge is required to attend this session; you only need to have completed the baseline construction questionnaire.</td>
</tr>
</table>

<table>
<tr>
<td>Minute 2.

Security
and
and risk management
Session #1: Introduction to digital security for non-governmental organizations (NGOs) &amp; human rights defenders
2025
Funded by the European Union
1</td>
<td><b>Facilitator Activity/Action</b>
Introduction to the topic</td>
<td><b>Strategy/Methodology</b>
Story about a generic visual</td>
</tr>
<tr>
<td colspan="3"><b>Script/instructions</b>
4. Yes, digital security is a complex topic that we have heard about, but about which we probably do not have in-depth knowledge. Don't worry, the idea is to take a practical approach to this complexity in order to learn how to protect ourselves when we inhabit and use digital media.
5. We can start by simply defining digital security as the set of practices, tools, and knowledge that protect personal information, devices, and communications in digital environments to prevent unauthorized access, data theft, cyberattacks, or undue surveillance.
6. In other words, digital security seeks to enable people to use technology safely, privately, and with confidence. As you can see, people are at the center of the idea of digital security.
7. Let 's get started!</td>
</tr>
</table>

<table>
<tr>
<td>Minute 4

Digital security and risk analysis
1 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.
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.
3</td>
<td><b>Facilitator Activity/Action</b>
Introduction to the topic</td>
<td><b>Strategy/Methodology</b>
Story about a descriptive visual</td>
</tr>
<tr>
<td colspan="3"><b>Script/instructions</b>
8. Course objectives: 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.
9. In this course, we will approach digital security from a risk analysis perspective. In the first session, we will understand the digital environment, especially the actors involved and the threats they face. In the second session, we will focus on thinking about the topic from the perspective of organizational communications, and in the third session, we will devote ourselves to thinking about a basic plan that will allow them to improve everyday practices and thereby improve digital security.</td>
</tr>
</table>

Minute 6  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 risks, threats, vulnerabilities, and capabilities that NGOs and human rights defenders face when using such tools. ✓ Identify the digital tools we use most.	**Facilitator Activity/Action** Introduction to the topic	**Strategy/Methodology** Story about a descriptive visual

Script/instructions

10. During this first session, we will focus on providing tools so that course participants can analyze and identify how the Internet works, and especially what role Internet intermediaries play in this ecosystem. This information will be key to evaluating and identifying how the tools we use daily on the Internet work and will allow us to establish the risks, threats, and vulnerabilities, as well as the capabilities we must develop within our organization to use these tools more securely.
11. By the end of this session, you will be able to analyze and identify how the internet works in general and the role of intermediary companies in this network. You will have tools to evaluate and identify the digital services you use most in your organization and will be able to identify the most common risks, threats, or vulnerabilities faced there.

Minute 8 **Digital security is a collaborative effort and a shared responsibility**	**Facilitator Activity/Action** Introduction to the topic	**Strategy/Methodology** Story about a descriptive visual

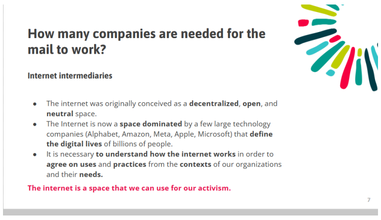
Script/instructions

12. Learning more about digital security and understanding that it is not an issue exclusively for the government, the private sector, the media, academia, or civil society allows us to affirm that digital security is a shared responsibility in which collaboration is a necessity.
13. Those of us participating in this course understand that the digital transformation of our societies has also meant an increase in threats to digital security. For example, the report "Global Trends in Digital Security: Civil Society and Media" published in 2023 by Internews recognizes that the scale and scope of digital threats facing civil society are related to geopolitical instability and events that depend on local contexts such as elections and protests, among others. https://internews.org/resource/global-trends-in-digital-security-civil-society-and-media/ (all the links I mention will be in the final slides for your reference).
14. This will only increase if we consider that we are constantly introducing new technological tools to facilitate the work of our organizations, which also results in the emergence of new types of threats and the re-emergence of more traditional ones.
15. In conclusion, all sectors and all individuals have a role to play in improving individual and collective protection.

Minute 10	**Facilitator Activity/Action**	**Strategy/Methodology**
 1. **How the internet works**	Begin the first content topic of Session 1	Story about a generic visual

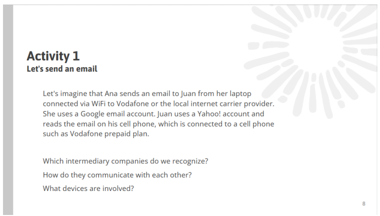
Script/instructions

16. The first thing we need to know is that, unlike other spaces we inhabit, the internet is a network in which private companies play a crucial role. All our activity depends on multiple actors who enable it to function. Some of these actors are public, but most are private companies. The operation of the internet at the international level falls almost exclusively to private companies and is highly concentrated. The role of the public sector is essentially regulatory. Therefore, the first thing we will do is investigate a little about how the internet works.
17. Warning: This explanation is not exhaustive, but rather aims to be a brief but direct overview of the role of internet intermediaries. For more complete information on the subject, you can check out online courses such as How the Internet Works? hosted by Stanford University at [https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm.](https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm)

Minute 12	**Facilitator Activity/Action**	**Strategy/Methodology**
 **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.** 7	Begin the process of explaining how the internet works, focusing on intermediary companies.	Narrative about a descriptive visual containing the text to be repeated. Then explain with examples the concept of "intermediaries" as private companies that enable us to carry out activities on the internet.

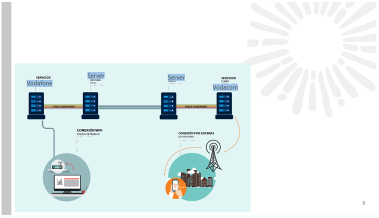
Script/instructions

18. *Read the slide*

Minute 15	**Facilitator's activity/action**	**Strategy/Methodology**
 **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? 8	Facilitate a practical exercise with the course participants.	Narrative about a descriptive visual containing the text to be repeated

Script/instructions

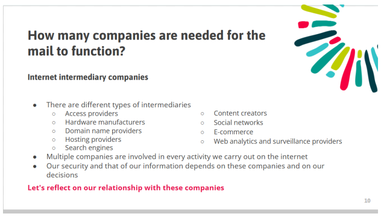
19. To better explain how the internet works from the perspective of intermediary companies, we will do an activity in which we follow step by step what happens when we send a message.
20. *Read the slide*

Minute 17	**Activity/Facilitator action**	**Strategy/Methodology**
 SERVIDOR Vodafone Server GOOGLE EEUU Server YAHOO SERVIDOR CLARO Vodacom CABLE SUBMARINO CABLE SUBMARINO CONEXIÓN WiFi OFICINA DE TRABAJO CONEXIÓN POR ANTENAS DESTINATARIO 9	Facilitate a practical exercise with the course participants.	Story about a visual aid that seeks to illustrate

Script/instructions

21. The image shows the route taken by Ana's message.
22. At a minimum, Ana needs to connect her to the Internet service provider such as Vodafone and a Gmail email service to send that message, which passes through the servers of the two companies and is received by the servers of the two companies that Juan uses: Vodafone and Yahoo. Just like Ana, in order for Juan to read the message, he needs his cell phone data provider (Vodafone) to connect him to the network and Yahoo software to manage it.
23. In any case, these are only the most visible companies. We must be aware that the process is the responsibility of different organizations and involves different technical approaches. Thus, for example, Ana's everyday action of sending an email, in addition to the Internet service provider and the email service provider, can be more complex:
    - If the email address corresponds to a proprietary domain, it must have been purchased from a domain seller; if the email is self-hosted, there must be a server where these emails are stored, and so on. Several services may be offered by the same company. Google, for example, could offer the email service, its storage, and usage analytics.
    - Additionally, when the message travels through the communications infrastructure to reach its destination, it connects through different operators and passes through different physical infrastructure, cables, modems, cell phone antennas, and national and international cables. All these steps, which for each person take only a few moments, are instances in which our message can be attacked, and both our precautions and the measures taken by these companies contribute to making the transit of information more or less secure.

    SUGGESTION: Depending on the skills of the facilitator, the exercise can be done by asking people to collectively trace the route shown in the drawing and described in the previous paragraph.

Minute 23	**Facilitator Activity/Action**	**Strategy/Methodology**
 **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** 10	Facilitate a practical exercise with the course participants.	Narrative about a visual that describes the activities

Script/instructions

24. The exercise involving the message sent by Ana to Juan shows some of what happens behind the scenes when a message is sent. This complexity is present in every activity we carry out on the internet—whether it be searches, payments, video calls, etc.—and involves a process mediated by multiple companies that contribute to the security of our activities in general, and our communications in particular. For example, when companies take steps to encrypt our messages or their channels take steps to protect our communications, if we also take the precaution of using stronger passwords, we are also contributing to that digital security.
25. From a risk analysis perspective, it is important to reflect on the activity we are carrying out, where we are doing it, and who is involved. This allows us to be more aware of the actions companies take to protect us,

the measures they offer to strengthen our security, and the practices we can incorporate to better mitigate risks.

26. *SUGGESTION: The facilitator can invite people to identify other intermediary companies. Here is a list of different types and the activities they do, with their trade names:*

Type of intermediary company	Activity	Example
Access Provider	Enable Internet connection	Claro, Movistar, AT&T, Vodafone
Hardware manufacturers	Design and maintain physical equipment and operating systems that facilitate information processing and Internet access	Apple, Huawei, LG
Domain name provider	Assign Internet domains	GoDaddy, NameCheap
Hosting	Information about web hosting	AWS, Wix, Greenhost
Search engine	Facilitate the aggregation, exchange, and search of information	Google, DuckDuckGo
Content creators	Producing their own content and regulating access	Netflix, Spotify, The New York Times,
Social networks	Connect users and communities	Meta, Google Workspace, Reddit
E-commerce	Selling goods and services and facilitating transactions	Amazon, Mercado Libre, eBay
Web analytics and surveillance	Collect data, adapt it for new purposes, and sell it	Google Analytics, Cellebrite

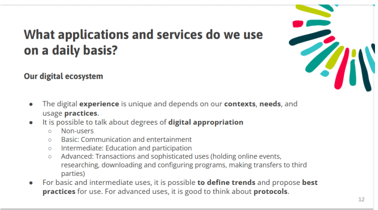
27. *At the end of the activity, the facilitator should make sure to highlight the conclusions on the slide:*

- 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

Minute 30	**Facilitator's activity/action**	**Strategy/Methodology**
 2. Inventory 11	Begin the second content topic of Session 1	Story about a generic visual

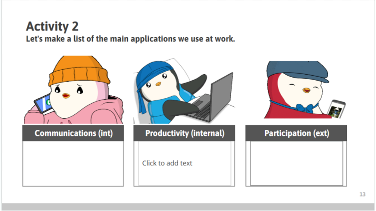
Script/instructions

28. Having established the central role played by private companies, the second topic we will address in this session is identifying the tools that people in NGOs and human rights organizations currently use in the digital environment. We will now focus on this.

Minute 30	**Facilitator's activity/action**	**Strategy/Methodology**
 **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**. 12	Develop the second content topic of session 1	Descriptive visual narrative

Script/instructions

29. *Read the first part of the slide*
30. *Expand on the last paragraph:* A practical way to address the risks involved in using tools in an organization is to create documents that explain best practices to people. In this regard, for the most basic and intermediate uses, it is possible to define trends and propose best practices for use. For advanced uses, it is a good idea to think about protocols that provide more details and elements to guide people in their use.
31. Identifying the tools we use most and the type of use we give them in our organizations is key to learning how to manage our digital security risks, which is why it is important to make an inventory.

Minute 33	**Facilitator Activity/Action**	**Strategy/Methodology**
 **Activity 2** **Let's make a list of the main applications we use at work.** Communications (int) Productivity (internal) Click to add text Participation (ext) 13	Develop the group activity for the second content topic of session 1.	Overview narrative

Script/instructions

32. We are going to carry out an exercise to collectively make a list of tools that we use in our daily work in organizations. Everyone should think about which ones they use most, considering the following three groups.
    - Internal communication tools (email (Gmail, Proton, Riseup, etc.), instant messaging (WhatsApp, Signal), video calls (Zoom, Meet)

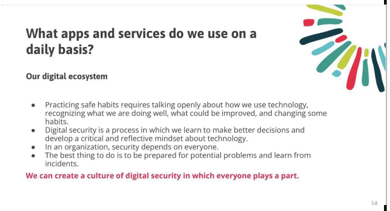
- Internal productivity tools such as Google Docs, Notion, Base Camp
- External participation tools: websites (CSS, WordPress), social media (Twitter, Instagram, LinkedIn)

33. You can call out the names of the tools or type them into the chat, and the slide will be filled with names.
34. The main idea is to make us aware of the tools we use and also to think about how we use them with different people and how they serve different purposes.
35. Depending on the tools mentioned, you can talk in general terms about their characteristics, which company is responsible for them, how much we depend on a single company or not, what characteristics differentiate them from each other, why we choose some and not others, what kind of data they expose about ourselves, our organization, or third parties, and so on.

Minute 48-58 BREAK	**Facilitator Activity/Action** Rest	**Strategy/Methodology** Stop for 10 minutes

Script/Instructions

36.

Minute 58  **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.** 14	**Facilitator's activity/action** Reflect on the group activity for the second content topic in Session 1	**Strategy/Methodology** Story about a descriptive visual

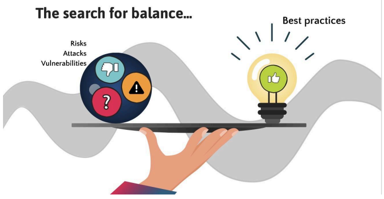
Script/instructions

37. *Read the key slide from the exercise done before the break, connecting it to any discussion that may have been sparked.*
38. In the second session, we will focus on communication tools and explore their risks in greater depth.

Minute 60 3. Risk analysis 15	**Facilitator's activity/action** Introduce the third topic of session 1.	**Strategy/Methodology** Description of a generic visual

Script/instructions

39. Since digital technology is now an important and useful part of our lives, we need to learn how to use it and manage the risks that arise from its use. In this section, we will learn how to perform a risk analysis that will enable us to manage those risks.

Minute 61	**Facilitator's activity/action**	**Strategy/Methodology**
 **The search for balance…** 	Present the third content topic of session 1	Story about a descriptive visual

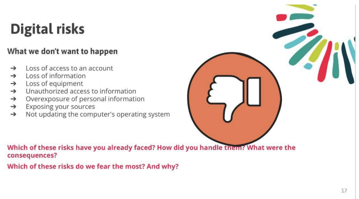
Script/instructions

40. Finding the balance between the benefits these tools offer and the risks, threats, and vulnerabilities they pose in these contexts is key to proper digital security management, which involves risk analysis on the one hand and the adoption of best practices on the other.

Minute 63	**Facilitator Activity/Action**	**Strategy/Methodology**
	Present the third content topic of session 1	Story about a descriptive visual

Script/instructions

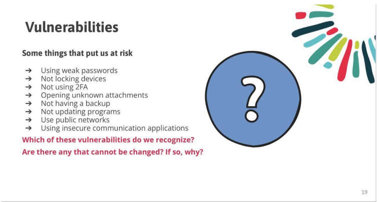
41. The slide shows the risks that we know most affect organizations such as yours.
42. *Read the slide*
43. *Use the questions to engage in a dynamic activity with those who want to respond and confirm that these types of situations have occurred. The idea is to encourage people to participate.*

Minute 67	**Facilitator's activity/action**	**Strategy/Methodology**
 **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?** 17	Present the third content topic of session 1	Story about a descriptive visual

Script/instructions

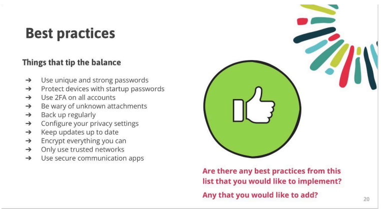
44. The most frequent attacks that result in the risks we saw are as follows
45. *Read the slide*
46. *Use the questions to engage in a dynamic activity with those who want to respond and thus confirm that these types of situations have occurred. The idea is to encourage people to participate.*
47. *SUPPLEMENTARY MATERIAL: The slide includes words that people may not necessarily know the meaning of. Here is a glossary that can be used to support the activity:*
    ***Phishing**: 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 (impersonation of a trusted third party) in order to manipulate them and get them to perform 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, doxxing, and doxeo[1] (Spanish adaptation) 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 in order 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 annoy or harass 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 their 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.*

Minute 75	**Facilitator Activity/Action**	**Strategy/Methodology**
 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? 19	Present the third content topic of session 1	Story about a descriptive visual

Script/instructions

48. The question is: How do we make these things happen? This is the moment when we need to talk about the main vulnerabilities we must avoid.
49. *Read the slide*
50. *Use the questions to engage in a dynamic activity with those who want to respond and confirm that these types of situations have occurred. The idea is to encourage people to participate.*
51. *Of the situations described there, it may be important for the facilitator to understand that 2FA stands for two-factor authentication or multi-factor authentication (MFA): more commonly known by its acronym MFA (Multi Factor Authentication), it is a method of computer access control in which a user is granted access to the system only after presenting two or more different proofs that they are who they say they are. In practice, this means that people are subjected to various tests, such as being asked for a known password and also a secondary key that rotates and launches an application, or a digital certificate installed on the computer, or providing biometric data, among other things (think of what most banks already ask for in order to carry out transactions).*

Minute 80	**Facilitator 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 Are there any best practices from this list that you would like to implement? Any that you would like to add? 20	Present the third content topic of session 1	Story about a descriptive visual

Script/instructions

52. So, what can I do? Once again, there is no way to guarantee 100% digital security, but we can improve our practices.

53. *Read the slide*
54. *Use the questions to engage in a dynamic activity with those who want to respond and confirm that these types of situations have occurred. The idea is to encourage people to participate.*
55. *Let's conclude by saying*: "But, consider this a preview, as this topic will be the focus of our third session, and we will return to it in the last session."

Minute 90

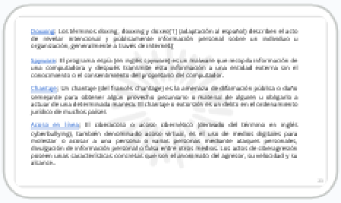
Glosario

Análisis de riesgo: El análisis de riesgo, también conocido como evaluación de riesgos o PHA por sus siglas en inglés: Process Hazards Analysis, es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir.

Intermediario de internet: Un intermediario de internet se refiere a una empresa que facilita el uso de internet . Entre estas empresas se incluyen los proveedores de servicios de internet (ISP), los motores de búsqueda y las plataformas de redes sociales.

Phishing: es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo, revelar información confidencial o hacer click en un enlace).

Explotación de vulnerabilidades: Las vulnerabilidades son fallos en los sistemas computacionales que pueden ser aprovechados (explotadas) por un atacante para realizar acciones no autorizadas que pueden comprometer la seguridad de la información contenida en los sistemas o el funcionamiento mismo de dichos sistemas.



Doxxing: Los términos doxing, doxxing y doxeo[1] (adaptación al español) describen el acto de revelar intencional y públicamente información personal sobre un individuo u organización, generalmente a través de internet.[

Spyware: El programa espía (en inglés spyware) es un malware que recopila información de una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del computador.

Chantaje: Un chantaje (del francés chantage) es la amenaza de difamación pública o daño semejante para obtener algún provecho pecuniario o material de alguien u obligarlo a actuar de una determinada manera. El chantaje o extorsión es un delito en el ordenamiento jurídico de muchos países.

Acoso en línea: El ciberacoso o acoso cibernético (derivado del término en inglés cyberbullying), también denominado acoso virtual, es el uso de medios digitales para molestar o acosar a una persona o varias personas mediante ataques personales, divulgación de información personal o falsa entre otros medios. Los actos de ciberagresión poseen unas características concretas que son el anonimato del agresor, su velocidad y su alcance.

Amenazas en línea: también conocida como ciberamenaza, es cualquier acto malicioso que busca comprometer la seguridad de sistemas informáticos, redes o dispositivos, con el fin de obtener acceso no autorizado, robar datos, causar daños o interrumpir operaciones.

Violencia digital de género: también conocida como violencia de género facilitada por la tecnología, se refiere a cualquier acto de violencia que ocurre en línea y que se dirige a personas por razones de género. Esta violencia se manifiesta a través de diversos medios digitales, como redes sociales, teléfonos móviles, plataformas de internet, y puede incluir acoso, amenazas, difusión de contenido íntimo sin consentimiento, entre otros.

Facilitator Activity/Action

Additional Resources Session 1

Strategy/Methodology

Additional resources that allow session participants to delve deeper

Script/Instructions

56. In the presentation you have access to, you will find a glossary that may be useful for future reference
57. See you at the next session!