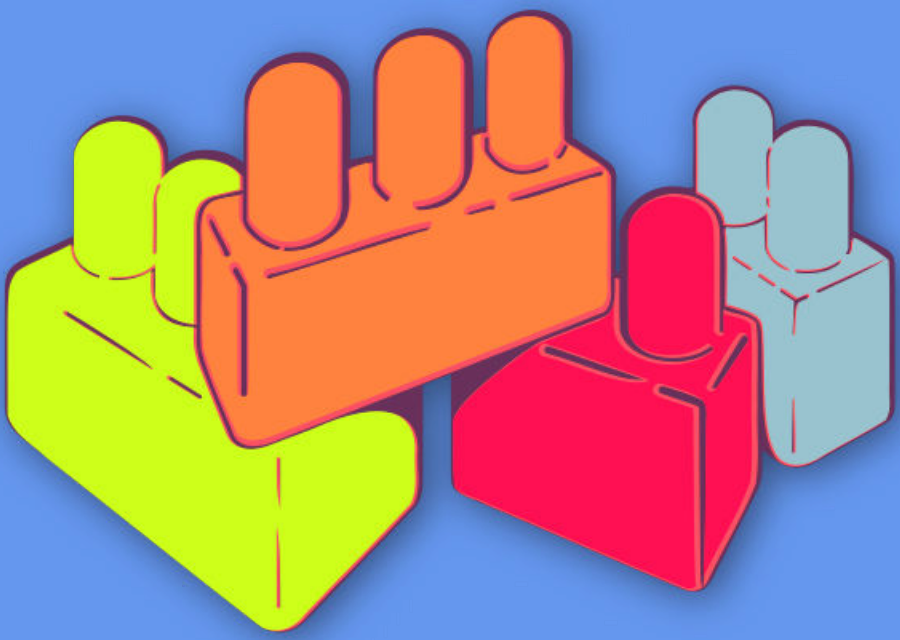
CYBERWOMEN



Digital security basics 1

Digital security basics 1

https://iwpr.net/

Contents

How does the internet work?

- **Objective(s):** Csharing an understanding the flow of information across the internet, and the different vulnerabilities and related good security practices at each point of the chain.
- **Length:** 60 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Who do you trust?[1]
  - Personal perceptions of security[2]
  - Your rights, your technology[3]
- **Needed materials:**
  - How Does the Internet Work? placards – these should be iconic representations of the parts of the chain that an email goes

[1] https://cyber-women.com/en/trust-building-exercises/who-do-you-trust/

[2] https://cyber-women.com/en/rethinking-our-relationship-with-technology/personal-perceptions-of-security/

[3] https://cyber-women.com/en/rethinking-our-relationship-with-technology/your-rights-your-technology/

through when it is sent from one computer to another: devices (computer/mobile phone) (x 2) (it's best for the computer and the phone to be on the same piece to avoid confusion.), modem (x2), telephone pole/underground optic fiber (x 2), internet service provider (x 2), Google servers (x 1), mock email (x 2, o más)
  - Handouts with suggestions of digital security practices
  - Paper to use as a board – one long piece (4 meters), and two smaller pieces (1 meter)
  - Colored markers
  - Adhesive tape
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
  - Speakers
- **Recommendations:** Make sure to cover all the questions participants might have. it is important they leave the session with answers to their concerns with the vulnerabilities they learned about, and feeling they have the information they need to take action. avoid creating an environment of fear, stress or anxiety - provide enough information and resources, as well as further training opportunities (if possible)

This session was developed jointly by Mariel García (SocialTIC) and Spyros Monastiriotis (Tactical Technology Collective)

Leading the session

Part 1 - How the Internet Works – Flow of Information and Points of Vulnerability.

1. This part of the workshop will begin as a game. Participants will be given pieces of paper representing one part of the chain of the flow of information online (modem, computer, ISP building, etc) and will be asked to arrange themselves in the order they consider is correct to represent the way an email travels through the Internet to reach another

computer.

2. Once the group is arranged, the facilitators will correct any mistakes, and will do a run-through explaining the process to everyone. Then a volunteer will be asked to repeat that explanation. It is recommended that the complete explanation is made at least three times; but, to give variety to this exercise, the facilitator can change the email illustrations that are used, and the extreme where the demonstration begins. The trainer must also give some time to clarify doubts related to this process.
3. You can also use a video like this one https://www.youtube.com/watch?v=7_LPdttKXPc to help participants identify any mistakes that they have in the way they arranged themselves.

   Optional: To adapt this for larger groups - rather than giving out one piece per person, assign one piece to a pair; for smaller groups, they can place the pieces on the floor, debating their order.

Part 2 - Vulnerabilities

4. When the previous process has been completed, participants will be asked to paste each piece on a long paper (from a roll) that will be left on the floor. At this point, the facilitators will go through the chain again, this time to point out and explain the vulnerabilities at each stage (and hint at good practices to keep participants calm and confident).

   Some of the vulnerabilities are mentioned next. You can also add any other practice or threat that is applicable in your own context or that is relevant to mention to the participants. You can also share a few examples of practices that other collectives you work with have to help participants think of what might be some of their own good or bad practices.

   Device 1 (computer/phone): Physical insecurity; loss of information

   Modem 1: Wifi sniffing; lack of encryption

Telephone pole/optic fiber underground: N/A

Internet Service Provider: Data and metadata requests from local/national governments

Google Servers: International surveillance; password insecurity and phishing, requests from national governments

Telephone pole/optic fiber underground 2: N/A

Modem 2: Security problems using other people's connections (like at Internet cafes)

Device 2: Malicious software; insecure deletion

Part 3 - Good Practices for Digital Security

5. After focusing on vulnerabilities, it will be time to break the group into smaller ones that can "adopt" one of the vulnerabilities discussed in the previous exercise and propose creative solutions for it. To make it less overwhelming for less experienced participants, each group will be given a piece of paper including one solution proposal that can ignite conversation.

   At the end, the groups will be given 30 seconds to a minute to present their ideas to the rest of the group (while one of the facilitators takes notes and makes additions to what is reported back by the groups). Facilitators will float around the groups giving brief explanations and answering questions, and mostly promoting discussion among all the participants.

   It's important that, as this activity progresses, facilitators explain the basics of each solution. Also, depending on the level of interaction and speed of the workshop, it may not be possible to cover all the proposals.

References

- https://securityinabox.org
- https://myshadow.org

Building stronger passwords

- **Objective(s):** In this session, you will review with participants the implications of a compromised password, how they are commonly compromised, and how to create stronger passwords and develop better password habits.
- **Length:** 45 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - How does the internet work?[1]
  - How to secure your computer[2]
- **Needed materials:**
  - Projector
  - Slides
  - Paper
  - WiFi/internet access to download KeePass

[1] https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/
[2] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/

This session is based on the module “Safer Password Practices” developed by Cheekay Cinco, Carol Waters and Megan DeBlois for LevelUp

Leading the Session

Part 1 - Introduction

1. Start this session asking participants:
    - When was the last time they changed any of their passwords?
    - Do they have different passwords for their different accounts?
    - Do they have their password written on a post-it note?
    - Do they have all their passwords stored on a document?
    - Do their phones have a password?

Part 2 - Why are Passwords Important?

2. Before you begin talking about the importance of passwords, ask participants to list all the information that is being kept safe through a password. What information do they have in their email accounts, social media accounts, cell phones? What would happen if someone else were able to access that information?
3. Now, share with the participants some reasons why passwords are important:
    - Passwords provide access to a number of important accounts such as email, banking accounts, social networking sites, etc.
    - These accounts often contain sensitive information, and also allow us to “be ourselves”, permitting organic interaction with others using various digital services - this might entail sending a social networking message, sending an email, making an online purchase, etc.

- They may also allow us to appear to be others - anyone with access to an account password can, in effect, act online as if they were the account owner.
- Passwords also provide access to a number of other things - Wi-Fi access points, unlocking mobile devices, logging-in to computers, decrypting of devices, files and more

Part 3 - What Can Happen If Your Password is Compromised?

4. In this part of the session we will share the papers with the participants and ask them to list all the platforms they can remember they have an account on. Now ask participants to list what might happen if someone had their password and could accessed their accounts or devices:
    - Important information or files could be stolen (copied) or deleted; if they are stolen, you may or may not realize it immediately. This could be anything from sensitive documents and files, to address book contacts and email messages.
    - Money and other funds could be stolen or spent, via access to credit cards or bank accounts.
    - Email or social media accounts could be used to send spam, or used to impersonate you or your friends, family, and colleagues.
    - Account access could be held in exchange for a form of "ransom" - this could include money, access to contacts, or access to other accounts.
    - Someone with a password could use this access to monitor communications and activities without your knowledge.
    - Access to your email could set off a "domino effect" where it is used to reset passwords to other accounts by requesting password reset links, eventually locking you out of many other accounts if the password remains unchanged.

Part 4 - How are Passwords Commonly Compromised?

5. Share some of the common practices that can end up with other people having access to your passwords:
    - When they are shared with others, or stored in an easily discoverable way - a commonly seen example is a computer login password written on a post-it note, and then stuck onto the same computer or nearby.
    - When someone witnesses a password being entered on your screen and writes it down or remembers it.
    - If using an email client without SSL (https) session-wide, only at the login page, this leaves passwords and other information vulnerable as they are visible by anyone with access to the connection after logging in.
    - A device is physically accessed, and passwords are able to obtained through “Save My Password” or “Remember Me” settings saved on websites via a browser - this is especially possible if full-disk encryption isn’t used on a device.
    - Malware, such as a keylogger which can document every keystroke on a device and send it to a waiting third-party, can reveal not just passwords but potentially a great deal more personal or sensitive information.
    - Platforms can also be hacked or vulnerabilities in their systems cause that their users information is exposed.

Part 5 - How Can We Make our Passwords Stronger?

6. Explain that if we use the same passwords for everything, and that password is compromised, all our accounts can be compromised. Share some qualities of safer, stronger passwords with the group:

Length: to put it simply – the longer, the better! 12 characters is a highly recommended minimum for strong passwords, and 20 characters is even better.

Complexity: use a password that's alpha-numeric, using upper and lower case letters, with a generous mix of numbers and special characters.

Changed Regularly: regularly change your passwords, particularly for your most sensitive accounts, and definitely change them if you receive an authenticated (not phishing) email telling you that a particular service has had user accounts and passwords compromised.

Using passphrases (imagine several passwords strung together into a "sentence" or phrase) is another example of a strong password practice – here are a few examples:

> NoALaMineriaEnAmericaLatina ("Say no to mining in Latin America")
>
> AbortoSiAbortoNoEsoLoDecidoYo (Abortion yes, Abortion no, that's for me to decide)
>
> NosotrxsNoCruzamosFronterasEllasNosCruzanANosotrxs (We didn't cross borders, borders crossed us)

7. Ask participants to take a few minutes to begin creating some examples of strong passwords. Remind participants that they should think about how sensitive the information is in a given account while they consider the length or complexity of their passwords – they may want to use their strongest passwords for their most important accounts, while using less complex (but still strong!) passwords for less important accounts.

References

- https://level-up.cc/curriculum/protecting-data/creating-and-managing-strong-passwords/input/safer-password-practices/

Malware and viruses

- **Objective(s):** This session addresses the basics of what malware is, and how user devices can become exposed to different kinds of malware, in the context of risks most typically encountered by women human rights defenders.
- **Length:** 30 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - How does the internet work?[1]
  - How to secure your computer[2]
  - Let's reset![3]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
- **Recommendations:** Ideally, this session will be followed by the "how to

[1] https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/
[2] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/
[3] https://cyber-women.com/en/digital-security-basics-2/lets-reset/

secure your computer" session, which is also in this module.

Leading the Session

Part 1 - Introduction to Malware

1. Explain to participants what malware is, and review a few of the types of malware that exist – at a minimum, it is recommended to cover the following:

    - Trojan Horse
    - Spyware
    - Ransomware
    - Keylogger

    Ransomware and keyloggers are increasingly common types of malware encountered by women human rights defenders in Latin America; if you are working with a group of women from that region, these will be important to address. Likewise, in general, make sure to include case studies and examples of malware that are commonly encountered in the context of the participants attending your training.

Part 2 - How Can You Get Infected?

2. Explain some of the most common ways that devices become infected with malware, and the unsafe practices that can lead to such infections. It is also important to explain the different purposes or motivations behind malware deployments:

    - Some malware is broadcast on a wide-scale with no particular target;
    - Other kinds are specifically targeted at activists, journalists or dissidents to gain access to their data or communications;

- Still other kinds are targeted at individuals known to be connected to a number of activists, journalists or dissidents in the hope of infecting multiple targets across a network.

Part 3 - Share Examples Involving Women & Women Human Rights Defenders

3. Finish the session by sharing examples of malware infection scenarios typically encountered by women and WHRDs; you can also share specific case studies involving women and WHRDs (from blogs, news or personal experience – always anonymize these unless you have explicit permission from the target to share their name)

   Here there are a few general examples of cases, and you might also know similar cases to these in your context as well:

   - A woman who received an email about an opportunity to get free tickets for a concert; the link within the email infected her smartphone with malware.
   - A woman activist that received a message from what appeared to be the email of a colleague; after clicking the link within the email, her computer hard drive "encrypted" and a message appeared on her screen requiring payment in order to regain access to her information.

Safe browsing

- **Objective(s):** Provide an introduction to safe web browsing practices, including an overview of plug-ins and other utilities that can be used to create a safer browsing environment.
- **Length:** 45 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - How does the internet work?[1]
  - How to secure your computer[2]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
  - WiFi connection

[1] https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/
[2] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/

Leading the Session

Part 1 - Choosing a Browser

1. Begin the session by asking participants which web browsers they use and what other options they have heard of. Present Firefox - explain the benefits of using it, and discuss briefly the difference between it and other common browsers such as Google Chrome or Internet Explorer.

   Optional: If working with Spanish speaking women, you might also find this video from Ella useful to begin the conversation: https://vimeo.com/109258771

Part 2 – Safer Browsing Practices

2. There are quite a few safer browsing practices to discuss that can be shared with participants – while you don't need to cover every single one of them, it is recommended to share enough to give your participants options (also remember to keep your content contextualized by sharing practices most relevant to participant context).
3. Explain to the group that you will be reviewing some safe browsing practices with them, but not yet focusing on specific tools other than the browsers themselves. Some participants might already be willing to change browsers, but others may not yet be – so before discussing more specific tools like browser plug-ins, it's important to keep the discussion grounded first in practice.

   Here are some example practices you can discuss:

   - Being vigilant of phishing and spear phishing attempts;
   - Blocking embedded ads and pop-up ads;
   - How cookies work – be sure to talk about how convenient they can be, but that they also have downsides;

- Disabling and erasing cookies from the browsers;
- Deleting browsing history;
- Not saving passwords in your browser settings;
- Checking the extensions that you add to your browser;
- Enabling the Do Not Track option in your browser;
- Google search alternatives (such as Duck Duck Go)
- Who implements online tracking and why? (Both https://trackography.org and https://www.mozilla.org/es-MX/lightbeam/ are good resources about this);
- Discuss HTTP versus HTTPS;
- What is a VPN (Virtual Private Network) and when should these be used?
- What exactly does Incognito Mode do, and when should it be used?

Part 3 – Tools and Extensions for Safer Browsing

4. Explain, now that you've addressed some basic practices for safer browsing, that you can also suggest certain tools – specifically browser plug-ins – which can help automate or otherwise facilitate adoption of some of these practices.
5. Present the following tools, explaining how each of them works, and remember to also share the links to download them with participants. It is essential that participants understand why each of the tools shared is important and useful; if not explained clearly, it can lead to participants making ill-informed decisions about their privacy or anonymity online.

Desktop Browser Tools

- No Script[3]

[3] https://noscript.net

- Adblock Plus[4]
- Privacidad Badger[5]
- HTTPS Everywhere[6]
- Click & Clean[7]
- Tor browser[8]
- Disconnect[9]
- uMatrix[10]

Mobile Browser Tools

- HTTPS Everywhere[11]
- Recursos de My Shadow[12]
- Orfox[13]
- Orbot[14]
- Tor for iPhone[15]

Other Practices & Features:

Incognito Mode (InPrivate Mode) This is a feature that frequently causes confusion as it is not well understood - participants might not have a clear understanding of how Incognito mode works as a browser feature, and when it is useful. Explain how Incognito (and similar) modes work, and offer some examples of when they can actually be helpful features to take advantage of.

[4] https://adblockplus.org/
[5] https://www.eff.org/privacybadger
[6] https://www.eff.org/https-everywhere
[7] https://www.hotcleaner.com
[8] https://www.torproject.org/download/download-easy.html.en
[9] https://disconnect.me
[10] https://addons.mozilla.org/es/firefox/addon/umatrix
[11] https://www.eff.org/https-everywhere
[12] https://mike.tig.as/onionbrowser
[13] https://mike.tig.as/onionbrowser
[14] https://mike.tig.as/onionbrowser
[15] https://mike.tig.as/onionbrowser

Safe Wi-Fi Practices

Finally, take some time to discuss, and if possible demonstrate, a few basic safe practices on for WiFi connections - this includes practices such as changing the default password of the modem, and showing participants how to monitor which devices are connected to their WiFi network.

Referencia

- https://myshadow.org/es/trace-my-shadow
- https://securityinabox.org/es/guide/firefox/windows
- https://securityinabox.org/es/guide/firefox/linux
- https://myshadow.org/es/tracking-data-traces
- https://cuidatuinfo.org/article/firefox-y-complementos-de-seguridad

How to secure your computer

- **Objective(s):** Identifying good practices to keep our computers safe.
- **Length:** 50 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - How does the internet work?[1]
  - Safe browsing[2]
  - Malware and viruses[3]
  - Storage and encryption[4]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
  - Printed copies of the Backup Format Template (see below)
- **Recommendations:** It is strongly recommended that you do live demon-

[1] https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/
[2] https://cyber-women.com/en/digital-security-basics-1/safe-browsing/
[3] https://cyber-women.com/en/digital-security-basics-1/malware-and-viruses/
[4] https://cyber-women.com/en/digital-security-basics-2/storage-and-encryption/

stration – using a projector connected to your laptop - of any tools you choose to cover in this session, so that participants can follow along and practice on their own computers using "dummy" files created for the purposes of the session (not actually important data or files!)

Leading the Session

Part 1 - Introduction

1. Ask participants how much they value their computers - How useful or essential is it to their personal and work lives? How much information they storage in their computers?
2. Now ask them - How much time do they spend on maintenance of their equipment? The difference between the degree with which people tend to value their devices versus the amount of time they spend on maintenance and care is often quite wide. Explain to the group that this session will focus on basic practices for protecting devices.

Part 2 – Physical Environments and Maintenance

3. Mention to the group that many practices related to device safety are in fact more related to physical security than digital security (this is a good way to reinforce the holistic focus of this curriculum). A good example of this is the importance of cleaning devices – to get rid of dirt or residue that might get inside – and to conduct regular physical inspections of equipment to identify any alterations or physical intrusion attempts. In that regard, you can recommend basic digital practices – like using a password to lock a device if they won't be in its immediate vicinity while it is switched on – as well as physical protections, such as using a keyboard protector or an anti-theft cable chain to prevent unwanted access or theft. Make sure to note here how the most critical aspect of their devices' physical safety: awareness. Being aware of

where a device is at any given moment – whether on their person, in the other room, or secured in another location – is essential!

4. Ask each participant to recall the details of their workplace - Which physical risks are present? Is their computer exposed to being stolen? Are there any misplaced cables? Is it possible that their computer might be exposed to extreme heat, cold or moisture? These are other important awareness points – physical awareness isn't just about making sure an adversary doesn't get ahold of their device(s), but also about the potential damage that a device's immediate environment might present.

Part 3 – Software Safety

5. Explain to participants the risks of using pirated software (high likelihood of downloading malware, can't regularly update in the same way as with licensed software, etc.); however, licensed software is also frequently quite expensive. Here, you can share a few resources with the group that will be helpful to address this:

   Osalt[5]

   Open a browser and navigate to Osalt – this is a website that presents free and open source alternatives to many major licensed software platforms and suites (for example, using Ubuntu instead of Windows; LibreOffice instead of Microsoft Word; Inkscape instead of Adobe Illustrator).

   TechSoup[6]

   Via TechSoup, human rights activists and their organizations may be eligible to receive free, or heavily discounted, versions of commercial software: users may look for official distributors among local ICT service providers and request for a non-profit or public sector license discount. A large distribution network for donated software is run by TechSoup - the link above contains a list of partners and the countries in

[5] http://www.osalt.com
[6] http://www.techsoupglobal.org/network

which they operate.

6. Explain to participants the importance of keeping all their software updated - first and foremost, it protects against security vulnerabilities. All software and updates should only be downloaded from trusted sources; for example, when updating Adobe Acrobat Reader, one should only use updates downloaded directly from Adobe, not third-party websites.
7. Next, explain to participants the importance of having an antivirus program on their computers - provide some background that can help demystify some of the common myths related to antivirus, such as:
    - Using two or more antivirus programs offers more protection.
    - Mac and Linux don't need antivirus software because they can't get viruses.
    - It's perfectly safe to use a pirated version of antivirus software.
    - Free antivirus programs are not as safe or reliable as paid programs.
8. Share these, along with any others that participants share with you – then, discuss some basic safe practices for using antivirus software and protecting against malware (see Malware & Viruses session in this module). Some useful ones to highlight here, in case you haven't already covered them in the Malware & Viruses session in this module, are:
    - Using the uBlock browser plug-in to avoid clicking on ads that might download malicious malware files onto their computer.
    - Being aware of phishing attempts, suspicious links or attachments found within emails in particular, that appear to be sent from unknown accounts or from accounts that appear similar to those of trusted contacts.
    - This is a good opportunity to mention firewalls – these offer an automated layer of protection in their computers. Share tools like

Comodo Firewall, ZoneAlarm and Glasswire. Newer (licensed) versions of Windows and Mac OS also have robust firewalls already installed.

Part 4 – Data Protection and Backups

9. Ask participants - How often do they backup their files? Share examples of best practices related to data backup, such as keeping the backup in a safe place that is separate from their computer, backing up their information on a frequent, regular basis and - depending on the information that is being backed up - to consider also encrypting the hard drive or storage media where data will be stored.
10. Share with participants the backup format template below, and have them start filling it in individually. Explain to the group that this is a useful way of creating a personal data backup policy – they can refer to this after the training, as a useful resource for keeping track of where their data is stored and how often that data should be backed up.

    Backup Format Template

Type of information
Importance/Value
How often it is produced or changed?
How often must it be backed up?

11. Explain next that, although there are backup automation tools available (such as Duplicati.com or Cobian), participants may find it easier to start doing their backups by manually dragging and dropping files to the backup storage media. This ultimately depends on the complexity or amount of data they have to manage – for the average user however, manual backups should be more than sufficient.
12. To follow-up on secure data backups, re-visit briefly the concept of encryption for storage media. Explain to the participants what it means

to do, and why encrypting their hard drives or storage media can be useful. **VeraCrypt and MacKeeper**, two relatively popular utilities for implementing file or disk encryption, could be mentioned here as options for participants to explore.

Part 5 - Deleting Files and Recovering Them

13. Read aloud the following statement:

    > From a purely technical perspective, there is no such thing as a delete function on your computer.

    Ask the group what they think about this – Does this statement make sense? How can it be that there is no such thing as a 'Delete' function? Remind the participants that they can drag a file to the Recycle Bin on their computer desktop, and then empty the bin, but all this does is clear the icon, remove the file's name from a hidden index of everything on your computer, and then tell their operating system that the space can be used for something else.

14. Ask the group - What do you think happens to the data that is 'deleted'? Until the operating system uses that newly free space, it will remain occupied by the contents of the deleted information, much like a filing cabinet that has had all its labels removed but still contains the original files.

15. Now explain that because of how a computer manages this storage space for data, if they have the right software and act quickly enough, they can restore information deleted by accident; likewise, there are also tools available that can be used to permanently delete files (not just remove them from the file index until the space is occupied). Take this opportunity to present **CCleaner, Eraser, and/or Bleachbit** as tools that can be used to delete files and Recuva as an option to recover deleted files.

References

- https://seguridaddigital.github.io/segdig/
- https://securityinabox.org/en/guide/malware
- https://level-up.cc/curriculum/malware-protection/using-antivirus-tools
- https://securityinabox.org/es/guide/avast/windows
- https://securityinabox.org/en/guide/ccleaner/windows
- https://securityinabox.org/en/guide/backup
- https://securityinabox.org/en/guide/destroy-sensitive-information
- https://chayn.gitbooks.io/Avanzado-diy-Privacidad-for-every-woman/content/Avanzado-pclaptop-security.html