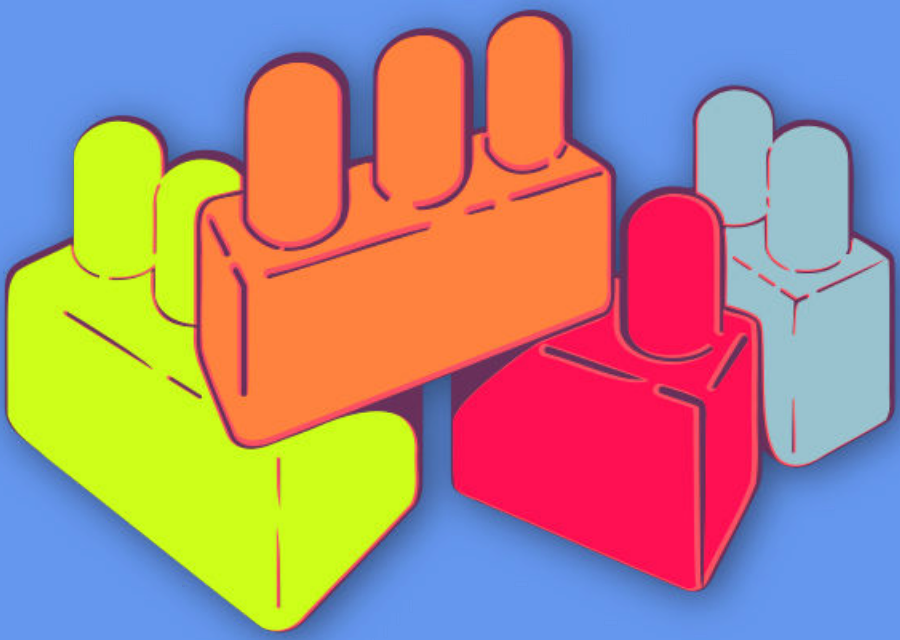
CYBERWOMEN



Digital security basics 1

Malware and viruses

https://iwpr.net/

Contents

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.