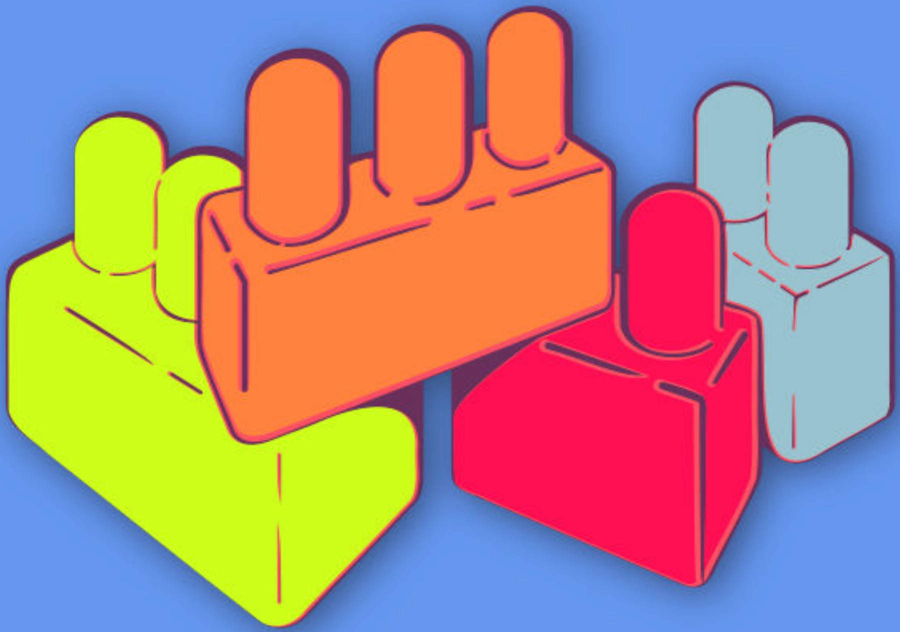
CYBERWOMEN



Digital security basics 1

How does the internet work?

INSTITUTE FOR
WAR & PEACE REPORTING

IWPR

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