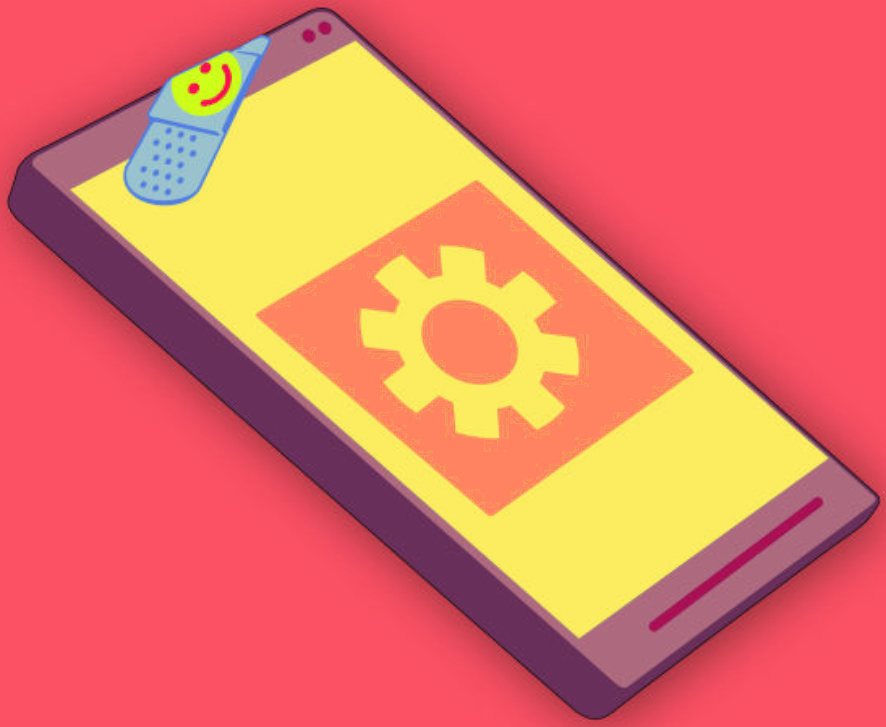
CYBERWOMEN



# Safer mobiles




https://iwpr.net/

# Contents

# Marco Polo

- **Objective(s):** Ideal for explaining to participants how a mobile phone works, and how we receive sms messages, phone calls and mobile data on our devices.
- **Length:** 15 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Networked publics[1]
  - Safe online campaigning[2]
- **Needed materials:**
  - Creativity!

This exercise is based on the "Marco Polo" exercise created by Fundación Karisma

[1] https://cyber-women.com/en/privacy/networked-publics/

[2] https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/

## Leading the exercise

1. Choose someone from the group to play the role of a “Mobile Phone” – once you have a volunteer, ask her to leave the room.
2. Using the space that you have, divide the rest of the group into “Buildings” and “Antennas” and ask them to distribute themselves throughout the room. Make sure that the antennas are spread evenly, so that each can define their own “quadrant” of the room.
3. Ask the Mobile Phone to come back into the room, and to close her eyes. Explain that she needs to locate all of the Antennas in the room by calling out “Marco” - the Antennas will respond with “Polo” but only if the Mobile Phone passes through their quadrant (the Buildings will remain silent).
4. Have the Mobile Phone attempt to locate all the Antennas by calling out “Marco” – once she has located all of them, you can now explain the basic functions of a mobile phone network:
    - Cell carriers operate antennas in different areas, each of which provides coverage for a specific zone (or quadrant);
    - Mobile phones receive coverage by sending out a request to new antennas they encounter (“Marco”) as they move from place to place, which antennas then reply to (“Polo”) by providing cell coverage.

# Mobile phones 1

- **Objective(s):** To provide participants with an introductory-level overview of how mobile devices function using mobile telephony networks.
- **Length:** 60 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Marco Polo[1]
  - Apps and online platforms: friend or foe?[2]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
  - Paper
- **Recommendations:** This session works best if it is done immediately following the marco polo exercise from this module; however, it can be

[1] https://cyber-women.com/en/safer-mobiles/marco-polo/
[2] https://cyber-women.com/en/privacy/apps-and-online-platforms-friend-or-foe/

done by itself as well.

This session is adapted from the activity “How Do Mobile Devices Work?” developed by Alix Dunn (The Engine Room) for LevelUp

## Leading the session

Begin by explaining participants the key parts of mobile phones. You can show pictures of each part while explaining them.

### Part 1 - What’s a Phone Made Of?

1. Although some phones, particularly smartphones, have much more advanced capabilities, all phones share several core components:

#### Antenna

Antennas, which permit communication between a mobile device and external networks, may be visible on older devices - some significantly older models requiring them to be pulled out manually for use. Most newer phones have the antennas built directly into its body, so they are no longer “visible.” Aside from the antenna responsible for communicating with the mobile network, there may also be antennas for WiFi; some manufacturers combine these functions into one antenna for the entire device.

#### Battery

A battery is what stores energy in order to power a mobile device; in most phones, batteries are easy to remove. In some newer smartphones (notably iPhones and later Samsung Galaxy S models), batteries are not designed for

removal and can be hard to access. Removable batteries are preferable for users who use tactics to increase their security.

**Baseband Microprocessor**

This component manages the communications of the phone, including the communications and commands from the user to the phone, and from the phone to and from the mobile network. The baseband of a phone is usually considered highly "proprietary" by manufacturers and can be considered a "black box" (inaccessible and not easily tampered with) in terms of its communication protocols, how they are controlled, and other network/device-specific functions. The capability of mobile networks to be able to turn on a phone, identify its location, listen via its microphone, and download data from the device is tied to the baseband on a device.

**SIM and SIM Slot**

This is where the SIM card is stored in a mobile device. There is a limited capacity for data storage on your SIM card, and some users can decide whether or not they want to save certain data to their SIM, internal phone memory, or to removable media. Mention that some phones are designed to manage multiple SIM cards; other phones operating on non-GSM networks (usually CDMA) do not have any SIM cards.

**Removable Media**

Removable media are any kind of external memory storage that can be inserted into and removed from a mobile device; these are usually SD-cards and micro-SD cards. Some phones also have Infrared (IR) ports for "beaming" data from one phone to another, as well as Bluetooth functionality.

**Cameras**

Most phones now have cameras that can take pictures and/or video, in particular smartphones. Many also feature cameras mounted to both the back and front of the device, frequently for use in tandem with video chat applications such as Facebook Messenger or Skype.

### Part 2 – Hands-On Practice

2. Ask participants to work in pairs and make a list of risks or threats that involve mobile devices; then, ask them to list some recommended practices they can think of to keep their mobile devices secure with respect to each of the components mentioned in Part 1 above.
3. Once each pair has finished working, ask them to present their solutions to the rest of the group. Listen for mentions of the following practices and tools in their presentations – if any of these aren't mentioned, make sure to include a brief explanation once everybody is done presenting:
    - Mobile Antivirus
    - VPNs
    - Checking apps configuration
    - Strong Passwords
    - Data Backups
    - Don't charge your phone via USB on public computers

## References


- https://securityinabox.org/en/guide/mobile-phones
- https://level-up.cc/curriculum/mobile-safety/how-mobile-networks-work/input/how-do-mobile-devices-work/

# Mobile phones 2

- **Objective(s):** Introducir herramientas y recomendaciones para mejorar la seguridad que tienen las participantes, ya familiarizadas con conceptos básicos de seguridad digital, con sus celulares.
- **Length:** 50 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Marco Polo[1]
  - Mobile phones 1[2]
  - Introduction to encryption[3]
  - How to secure your computer[4]
- **Related sessions/exercises:**
  - Marco Polo[5]
  - Mobile phones 1[6]

[1] https://cyber-women.com/en/safer-mobiles/marco-polo/
[2] https://cyber-women.com/en/safer-mobiles/mobile-phones-1/
[3] https://cyber-women.com/en/encryption/introduction-to-encryption/
[4] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/
[5] https://cyber-women.com/en/safer-mobiles/marco-polo/
[6] https://cyber-women.com/en/safer-mobiles/mobile-phones-1/

  - Apps and online platforms: friend or foe?[7]
  - How to secure your computer[8]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
- **Recommendations:** If possible, try to know before the training begins what kinds of phones participants use – for instance, this could be a question on a pre-training assessment survey. this will help you tailor your session content to the specifics of the devices/operating systems participants already use. before you start the session, remind participants of some basic digital security practices that can be implemented for mobile phones such as: mobile antivirus software, mobile vpns, checking app settings and permissions. **have participants perform a backup of the files they have on their devices before starting this session!** since they will be using their own devices for this session, it is important that they back their data up just in case.

# Leading the session

## Part 1 – Encryption for Mobile Devices

1. Remind participants of previous sessions that have touched upon the concept of encryption, especially the Introduction to Encryption session – you may have also discussed encryption previously in the context of full disk encryption during the How to Secure Your Computer session. Note to participants that the latest versions of iOS and Android (May 2017) now have encryption turned-on by default.

[7] https://cyber-women.com/en/privacy/apps-and-online-platforms-friend-or-foe/
[8] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/

### Part 2 – Using GPG on a Mobile Device

2. If participants are already familiar with GPG encryption, introduce them to the K-9 email client and to APG. Discuss the pros and cons of using GPG on a mobile device (especially the risk of keeping a private GPG key stored on a smartphone versus the unique vulnerabilities of mobile devices) – the idea here is to reinforce that these decisions can vary from one context to another; participants will need to decide on their own whether the pros of using GPG on a mobile device outweigh the cons.

   **Optional:** Give participants time to install and practice using K9 and APG during this session - they may want to try using the new keypairs that they create as they get familiar with the tool.

### Part 3 - Is Your Phone Tracking You?

3. Ask participants - How much information do our phones know about us? Phones are a medium for many of our conversations, and thus have access to most if not all their contents; likewise, phones also keep track of not just content but also contacts – every conversation can be connected to specific individuals.
4. You may also want to discuss with participants how the kind of tracking a phone performs could be considered a form of surveillance, and how surveillance can take place through more than just the usual, anticipated methods. Ask the group about what kinds of threats or risks they feel might be posed by their mobile devices, specifically in the context of their work as WHRDs.

## References


- https://securityinabox.org/en/guide/mobile-phones

- http://www.zeit.de/datenschutz/malte-spitz-data-retention