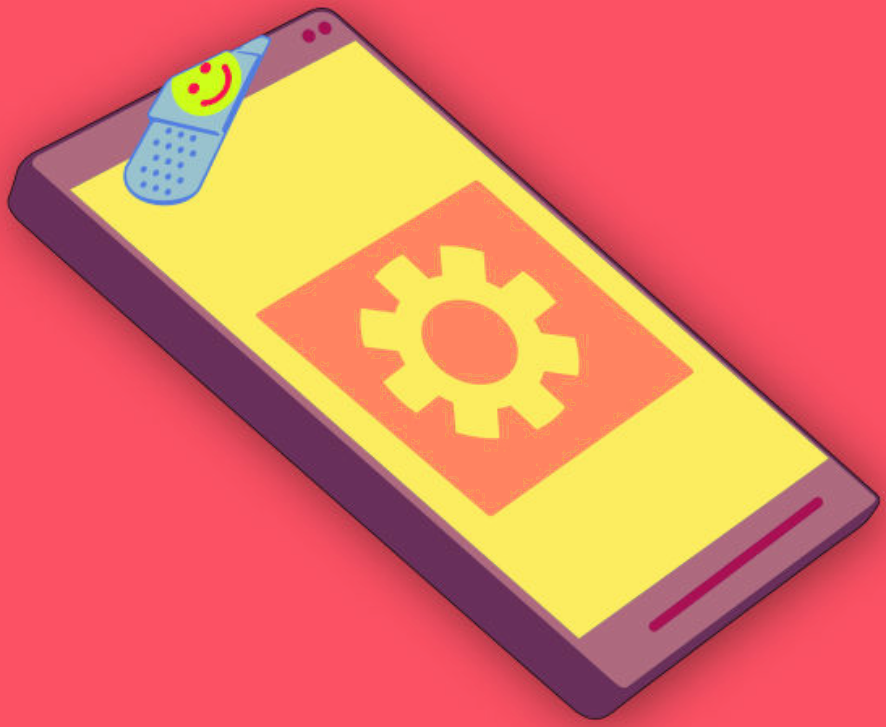
CYBERWOMEN



Safer mobiles

Mobile phones 1

https://iwpr.net/

Contents

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 done by itself as well.

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

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/