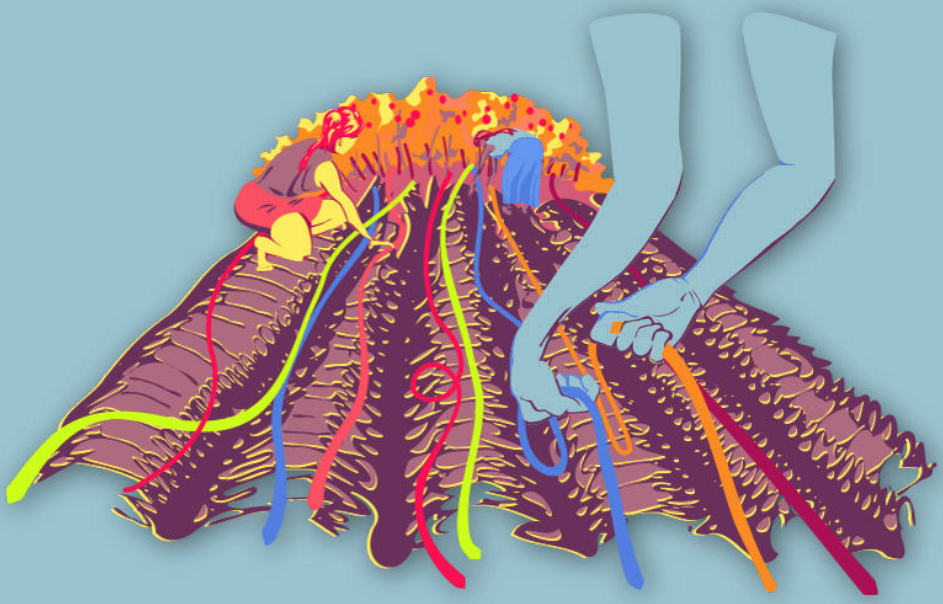
CYBERWOMEN



Determining the best solution

Digital security decisions

https://iwpr.net/

Contents

Digital security decisions

- **Objective(s):** To introduce women to the strategic critical thinking process that goes into making informed decisions about the implementation of digital security practices and tools, and to identify resources that will help them stay up to date after the training.
- **Length:** 90 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
- **Related sessions/exercises:**
  - Personal perceptions of security[1]
  - Who do you trust?[2]
  - How does the internet work?[3]
  - Apps and online platforms: friend or foe?[4]
- **Needed materials:**

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

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

[3] https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/

[4] https://cyber-women.com/en/privacy/apps-and-online-platforms-friend-or-foe/

  - Slides with key points included below
  - Laptop/computer and projector setup
  - Copies of WHRD case infographics (See Appendices)
- **Recommendations:** As this session requires a basic level of baseline knowledge of digital security concepts, it is best suited for a multi-day training or as part of a shorter workshop focused more on designing individual security protocols.

Leading the session

Part 1 - Introduction

1. Start by asking participants how many times they have asked a trainer or other expert a question about digital security, only to receive different answers each time depending on who they ask – it's quite confusing, right? Sometimes when we ask for advice on digital security, people who offer to help may not walk us through a process, but will just "fix the problem" on our devices without explaining what they've done – wouldn't you rather know what it is that they did so you can replicate the process if the problem arises again?
2. Explain that the goal of this session is to introduce the group to the strategic critical thinking process that goes into making informed decisions about the implementation of digital security practices and tools, and to identify resources that will help them stay up to date after the training. Discuss how digital security is about more than just downloading new apps, it is about knowing your practices well and making informed decisions to build a safer environment for yourself.

Part 2 – How Was Your Software Built?

3. Show or demonstrate once more to participants a few of the tools or platforms that you might have presented previously to the participants

(e.g. Signal, HTTPS Everywhere, ObscuraCam, Skype, Telegram, etc.) – ask them to identify which type of software each one is according to the information they have access to, such as a tool's website.

4. Explain what proprietary (closed source) software is: what are the characteristics of this type of software (provide examples of programs). What are the digital security implications of using this type of software?
5. Explain what open source software is: what are the characteristics of this type of software (provide examples of programs). What are the digital security implications of using this type of software? Be sure to also explain the open source software community and software auditing for context.
6. Explain what FLOSS (Free/Libre and Open Source Software) is: what are the characteristics of this type of software (provide examples of programs). What are the digital security implications of using this type of software?

Part 3 – Thinking About Users

7. If you've already covered the session Who Do You Trust? from the "Rethinking Our Relationship with Technology" module, remind the group of the examples of adversaries they shared; likewise, if you already covered the Gender Based Risk-Model exercise, remind the group of the risk model you created together.
    - This is all to ultimately reinforce that that not everybody has the same needs or faces the same risks in terms of digital security:
    - When looking for a digital security solution, learn as much as you can from the specific need you've identified. What is it you want to do or make more secure? Where is the safest or more secure place to keep something? From whom does it need to be protected?

- Consider the platforms or tools that you already use - How willing or possible it is for you to change those out for new platforms or tools, or to change the way you use your current ones?
- To what extent does connectivity have an impact on a potential digital security solution? Do you generally have consistent, reliable access to an internet connection, or do you need to be able to work without one for extended periods?
- If you're considering a digital security solution for an organizational or collective context, consider the different devices or operating systems that people within that group are using – Will the solution work for everybody? Will it work for a majority of people?

Part 4 – Thinking About Tools

8. The following questions are important ones to ask when considering using a new platform or tool – explain this to participants. You don't need to go through and answer each one individually (as they are very specific), but be sure to read them out loud and give a bit of background for why each is important:
    - Is it free and open source software?
    - Do you know who coded the tool, or who funded the project?
    - Is it available in my language?
    - Search for blogposts or mentions of the tool online, what do you find?
    - When was the last update of the tool?
    - Is it a stable version of the software?
    - Is someone providing support for the tool, or is it being supported by volunteers?
    - How easy is it to configure?
    - Has it been tested or audited?
    - Is the tool available for the operating system you use on your device(s)?

- Check the Terms of Service of the tool – do you agree with them, or do they seem suspicious?
- If the tool or platform uses remote servers, do you know where they are located?
- Have the developers ever handed over user data in response to a government request?
- How is the information stored in their servers? Is it encrypted, and if so does the project have a way of decrypting and accessing it?
- If you have any doubts, see if there is a way to contact the developers directly and get in touch.

9. Remind the group once more that there is not one universal digital security solution or recommendation for everybody - not all tools will be proper fit for every user. Being strategic about digital security tools and practices is more about getting to know ourselves better as users, choosing which tools work best for each of us based on our knowledge of our own circumstances.

10. Point out to the group that a lot of digital security software incorporates encryption to varying degrees – explain to participants that if encryption is an important feature for them, then open-source software is recommended. Open source software can be audited by the community to ensure that there are no backdoors; if a given tool's software does not incorporate encryption, and encryption is not an important factor in decision making, the use of open-source software may be less important (though certainly cheaper).

11. Complete this part of the session by having participants split up into groups of 3-4 people (maximum) – in their groups, ask them to make a list of some digital security tools they know, and to answer the questions listed about each one. As they go, each group should discuss the advantages and disadvantages they find within in each of the tools they listed – give participants about 10-15 minutes for this step, with each group sharing their outcomes once time is up.

Part 5 – Practice Thinking of Solutions

12. Provide participants with the set of WHRD case infographics (See Appendices) and ask them to remain in their groups from the previous step – make sure you have enough cases to give one to each group. Don't share the solution component with the groups – during this step, participants should work together to come up with their own solutions based on the information they have been provided during this session and what they might already know about digital security tools.

Part 6 – Resources for Staying Up to Date

13. It's important for your participants to have access to further resources once the training is complete, that they can refer to in order to maintain their practice and to keep themselves updated on new tools or practices that emerge from the digital security community.

    Here are some suggested resources which you can offer to your participants:

    - Zen and the Art of Making Tech Work for You // Tactical Technology Collective[5]
    - Security in a Box // Frontline Defenders & Tactical Technology Collective[6]
    - Surveillance Self-Defense // Electronic Frontier Foundation[7]
    - Genios de Internet // Spanish // Karisma Foundation[8]

    Optional: You may also list out different organizations that participants can follow (generally online, on Twitter, etc.) to get access to further digital security in their countries.

[5] https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual
[6] https://securityinabox.org
[7] https://ssd.eff.org/en/module/choosing-your-tools
[8] https://karisma.org.co/genios-de-internet-una-guia-para-mejorar-tu-seguridad-en-la-red/