CYBERWOMEN

Rethinking our relationship with technology

Your rights, your technology

https://iwpr.net/

Contents

Your rights, your technology

- **Objective(s):** This session involves a discussion about the relationship between rights and technology – you will then help participants identify current threats to their rights and then introduce them to some basic, relevant digital security concepts.
- **Length:** 50 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Personal perceptions of security[1]
  - Who do you trust?[2]
  - Introduction to encryption[3]
  - Anonymity[4]

[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/encryption/introduction-to-encryption/

[4] https://cyber-women.com/en/anonymity/anonymity/

  - Privacy[5]
  - How does the internet work?[6]
  - A feminist internet[7]
- **Needed materials:**
  - Flipchart paper
  - Colored markers
  - Copies of reports and news about digital rights from participants' home country(ies) or region(s), (one copy for every 3-4 participants)
- **Recommendations:** The references section of this session includes links to organizations that regularly publish reporting on digital rights issues. for the reports you select, make sure they cover a range of specific rights issues such as surveillance, internet shutdowns, content censorship and other examples of threats that are commons in the country or region.

Leading the Session

Part 1 – Connecting Rights with Technology

1. Split participants up into groups of 3-4 people (maximum), and give each group 1-2 large sheets of flipchart paper and some markers. Each group will have 10 minutes to brainstorm a list of human rights – how each group defines this is up to them. They should write these down on their flipchart paper.
2. Once the 10 minutes are up, you will then ask each group to look at the list they've made – they should now take another 10 minutes to discuss how these human rights are connected to technology (for example, "what impact does technology have on our human rights?"). To

[5] https://cyber-women.com/en/privacy/privacy/
[6] https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/
[7] https://cyber-women.com/en/online-violence-against-women/a-feminist-internet/

demonstrate, you can provide an example by drawing such a connection between technology and a human right listed by one the groups. They can write these down on another sheet of flipchart paper if they so choose, but it is not required.

3. Once the next 10 minutes are up, share with each group a pre-prepared packet of digital rights reports and news (see Needed Materials). Giving each group another 15 minutes, ask them to read through some of these and then brainstorm corresponding digital/online threats to the human rights they listed during Step 1. Explain to participants that the reports you've provided are just a guide - if they know of other cases or threats, they can include those as well.
4. Once the final 15 minutes are up, pause and then ask each group to briefly present their work to the rest of the participants.
5. Once each group has presented, begin a conversation with participants about how it can be easy for women human rights defenders to feel overwhelmed or helpless when confronted by the different risks and threats they may face online - if you already had this discussion during the Personal Perceptions of Security session from this module, you may simply remind them of that discussion.
6. Make sure that you've left enough time (15-20 minutes should suffice) to close this part of the session by providing some examples of practices or tools that are available to counter these threats. If you've already done the "Personal perceptions of security" session from this module, remember to also consider the motivations, resistances and barriers identified by participants when making recommendations.

Part 2 – Digital Security and Digital Rights Concepts

7. Now that you've covered some basic digital security practices and tools in response to the online/digital threats to human rights discussed during Part 1, explain to participants that you will now introduce a few core digital security concepts with concrete implications on rights:

anonymity, privacy and encryption. In some contexts, it might be important to also include circumvention as one of these examples.

8. Start out by reminding participants how important it is that they are taking this critical step towards addressing their own digital security with this training, and that now they will begin the process of learning how to counter some of the threats they face:

    - If you've already covered the session Personal Perceptions of Securityfrom this module, recall some of the perceptions and definitions of digital security that participants shared during Steps 2, 3 and 4 of that session.

    - If you have not already covered the session Personal Perceptions of Security from this module, it will be good idea here to now discuss with participants what digital security means in a broad sense, based on your own expertise.

9. Ask participants to volunteer their own definitions of what privacy means to them, and follow-up by then asking them how they feel about the current state of privacy on the digital era. Next, explain what digital/online privacy is – as you explain this, make sure to find ways of actively encouraging participants to reclaim their right to privacy.

10. Repeat Step 9, but this time addressing the concept of anonymity - ask participants what anonymity means to them, and briefly explain or clarify any doubts using examples as possible or appropriate. Again, find ways of actively encouraging participants to reclaim their right to anonymity, and be sure to also make clear what the differences are between privacy and anonymity as distinct concepts.

11. Once you have finished the above discussions and explanations of privacy and anonymity, move on to introduce encryption – explain how this will be one of the concepts they will learn during the training, and that some of the practices and tools you will cover during this training incorporate encryption in different ways. Briefly overview what some of these practices and tools are, drawing connections between these and the earlier discussions of digital rights, privacy and anonymity.

12. To conclude the session, suggest a few organizations that provide support and advocacy for digital rights in the participants' home country(ies) or region(s), so they can research and become familiar with them on their own – for instance, if working with a group from Latin America you can include organizations like Derechos Digitales, R3D, Global Voices, Karisma or Access Now.

References

- https://www.derechosdigitales.org
- https://r3d.mx
- https://karisma.org.co
- http://acceso.or.cr
- https://articulo19.org