CYBERWOMEN

Rethinking our relationship with technology

Rethinking our relationship with technology

https://iwpr.net/

Contents

Personal perceptions of security

- **Objective(s):** Here you will introduce the concept of holistic security to your participants, each of whom is carrying their own personal motivations, resistances, barriers and pre-conceived notions related to digital security, gender and technology into the training room - this session will encourage participants to identify what these could be, and to consider what the idea of "security" means to them individually.
- **Length:** 90 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Who do you trust?[1]
  - Your rights, your technology[2]

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

[2] https://cyber-women.com/en/rethinking-our-relationship-with-technology/your-rights-your-technology/

  - Gender-based risk model[3]
- **Needed materials:**
  - Sheets of lined or un-lined A4 paper (several per participant)
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
  - Flipchart paper

Leading the session

Part 1 - What is Safety for You? What is Security for You?

1. Ask participants split up into small groups of 3-4 people (maximum), giving them 15 minutes to discuss the following questions with each other:

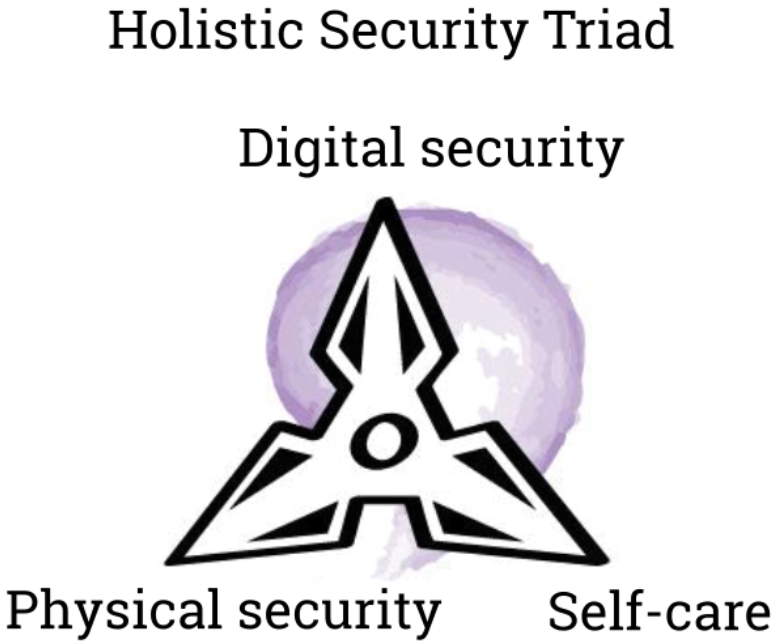
   - What is safety for you?
   - What is security for you?
   - What makes you feel safe and secure?
   - Which scopes do you think this concepts can apply to?

   For the above questions, keep in mind that some languages may not have equivalent words for both “safety” and “security” or they may use just one word to refer to both concepts.

2. Next, on projected slides or on flipchart paper, introduce participants to the holistic approach of the training. Take care to explain the importance of digital security, self-care and physical security to the holistic process (you can use or replicate the following graphic as a simple way to illustrate this):

3. In many cases, you may be working with participants who are taking part in the training so they can implement measures within their own organizations; therefore, it is important to explain to the group that this training process will be addressing security in the individual as well

[3] https://cyber-women.com/en/determining-the-best-solution/gender-based-risk-model/



Holistic security triad

as the collective contexts. Organizations and collectives are made up of individuals – to address security in a holistic manner, we need to first look at ourselves, then the networks and roles we occupy within an organization or collective, and then finally at the organization or collective itself.

Part 2 - What Does Digital Security Mean to You?

4. Ask each participant to think of what digital security means to them – ask them to write down a few sentences describing their own personal concept, working individually. Before they begin working, explain that - depending on circumstances such as personal experience, priorities, cause/activism or country of origin - their concepts may vary from person to person (and may include other elements, such as certain legal restrictions, etc.). To help each trainee develop their own concept, you can start by sharing yours as an example.
5. Once time is up, ask the participants if they would like to share what they wrote with the rest of the group – there is no pressure for everybody to share however, as some participants may not necessarily feel comfortable doing so.
6. After a few volunteers have shared their concepts, highlight some of the key elements they have presented - explain to participants that above all else (and especially above tools and technology) digital security is about us as individuals and as humans - our habits, our devices, the networks and groups we are part of, the context we live in, the information we have and where we have it.

Part 3 - Identifying Motivations, Resistances and Barriers

7. In groups of 3-4 people (maximum), have participants discuss their motivations, concerns and barriers related to digital security by answering the following questions:

- Why do they want to learn more about digital security?
- What are their personal reasons to be here at the workshop?
- What are their expectations from this training?
- Do they have any personal resistances to digital security?
- What challenges have they faced with learning about digital security? Or, what do they feel has prevented them from learning before?

8. Once time is up, ask each group to share their thoughts and discussions with the rest of the room - as the trainer, this is a crucial moment for you. To adapt the sessions in your training in a way that is truly relevant to the context of your participants, it is extremely important that you pay close attention to the specific motivations, resistances and barriers shared by participants.

Part 4 – Digital Security, Gender and Technology Myths

9. For this part of discussion, prepare ahead of time to share more information on the below examples of commons myths and misconceptions about digital security, gender and technology. Apart from explanations based on your own expertise, be sure to also find ways to relate the discussion back to some of the motivations, resistances and barriers identified by participants in previous section:

   "Digital security is hard."

   Digital security is a process. As you begin to learn more about it, you are likely to discover several unsafe practices of their own: **don't stress yourself!** Don't feel that you must change all your habits in just one day (or even one training). That you are beginning this personal journey now is a positive, healthy step!

   The more progress you make, the more you will come to realize that there is rarely just one answer to most digital security questions. What is most important to recognize is that **you know yourself the better than anyone** (or anything) else; therefore, you are the one who knows

best what changes and new habits you will be able to introduce into your daily routine. It is better to start out with a practice that you feel you can realistically implement, rather than to set the bar too high and become discouraged.

> "Digital security about learning how to use a 'bunch of new tools' that none of my friends or colleagues are using."

In reality, many of the most basic and essential digital security practices **do not rely very much on digital security tools**. Periodically changing the passwords for your accounts, checking the privacy configurations of the accounts you already use, protecting your devices with passwords, and regularly backing up your data are much more about your own habits and behaviors than the technology or tools themselves.

The digital security process we are about to begin is about providing you with the information that you need to make your own informed decisions about your digital security – it is focused on learning more about the platforms we already use, the implications that choosing certain tools or practices may have on ourselves and our work, and about improving the ways that we already use technology in our everyday lives.

Together, we will work on improving these practices while learning more about the risks we face as we make these decisions and changes. We will learn and share information with each other that can help us make better decisions about which of our practices we need to change, and importantly, **which ones we are already doing well**. Most importantly though, you have the last word - **the decision is yours!**

> "Digital security tools are expensive."

Most digital security tools are actually **completely free** to use. The amount and variety of these tools available is increasing every day, and FLOSS (Free Libre and Open Source Software) projects are increasingly creating free tools that run on a growing number of desktop and mobile operating systems; likewise, many of the most popular platforms now

include easier to use security features.

> "I don't know anything about digital security!"

You may be surprised, but most of us have in fact already put a lot of thought into our practices without realizing it – for example, many of you already use passwords to protect your phone or your laptop; some of you might already use different apps or tools to communicate with others about certain issues; and a few of you may even use a pseudonym or separate identity for your work/activism.

Optional: For this myth in particular, it may be a good idea to take a few minutes and ask participants for examples of practices they are already implementing related to digital security. Write these down on a sheet of flipchart paper for the group and post it in a visible place to reference throughout the training.

> "I don't use (or barely use) the internet, so digital security doesn't matter."

Digital security isn't just about what you do online – offline practices, such as regularly checking what information (contacts, images, documents, audio/video files, etc.) you have stored on your computer, smartphone (and "non"-smartphones) and USB drives, as well as physical awareness of where your devices are or who has access to them, are just as important – even if you aren't connected to the internet. It is especially critical to be aware of which apps and software are installed on your devices – sometimes, to access certain information on our devices, we may have had to install new apps or create new accounts without realizing it.

> "I have nothing to hide, or if I do, it doesn't matter because the government (or whoever else) will find out anyway."

As explained in the Tactical Technology project 'Me and My Shadow':

> Privacy is not about hiding - it is about autonomy, power and control; it is about your ability to decide how you present yourself to the world

You may think that you have nothing to hide, but briefly reflect on what kinds of information you share: Who do you talk to or communicate with about it? Which channels do you use to do so? Are those channels public or otherwise open for everybody to read?

In one way or another, we make decisions about what kinds of information we share, and with whom we share it, every day. You also need to> consider that even if you have nothing to hide now, this could become the case in the future – you will want to be prepared that possibility!

Have you ever felt completely overwhelmed or defeated upon hearing about the digital surveillance or harassment tactics of governments or other groups against women human rights defenders? In the course of our activism, it is normal to have these moments, and not only in the context of digital security or online threats - this is why we are starting this holistic process! Together, we'll build a layered approach that can help us to protect ourselves and our information. This is something you can achieve!

Part 5 – Closing Affirmations

10. Close the discussion by suggesting some (or all) of the following ideas and encouragements to the group – again, consider the motivations, resistances and barriers identified by participants and choose accordingly:

- How can we overcome the obstacle of thinking "technology and me, we just don't get along quite well"?
- Tools and technology don't have magic superpowers over us! We are the ones who decide what we give them access to - and if something happens, we can always reset them!

- We alone are the only ones who know which digital security practices are most appropriate for us, and we alone are the ones who can best decide which are the best and most practical to implement.

Optional: If your training will include this as a desired output, this is an excellent time to explain to participants that, as you move forward together with the training process, they will write their own individual plans for which practices and tools they will implement. Such plans should also include personal goals that will encourage them to make progress at their own pace.

References

- https://myshadow.org/es/tracking-so-what
- https://ssd.eff.org/en/module/seven-steps-digital-security

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

Her-story of technology

- **Objective(s):** Provide participants an empowering look at the leadership of women throughout the history and evolution of modern technology, with the aim of dispelling damaging gender constructs involving women and technology.
- **Length:** 20 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - A feminist internet[1]
  - Witch coven[2]
- **Needed materials:**
  - Photos of different women in tech (with names)
  - Bio for each woman (for trainer reference)
  - A length of string or cord (about 1 meter/3 feet)
  - Clothespins or Alligator clips (1-2 for each photo)

[1] https://cyber-women.com/en/online-violence-against-women/a-feminist-internet/
[2] https://cyber-women.com/en/closing-and-review-exercises/witch-coven/

Leading the Session

1. Explain to participants that this session will be an exercise for the group to develop a collective memory that recognizes women technologists through history (or, her-story). Ask the group:

   How many times have we heard that women and technology are not a good fit together?

   How many times have we heard that our place is not in a public or academic space, but behind the scenes or out of sight?

2. Have the group sit in a circle (on the floor or in chairs) and begin the session with a brief introduction to the gender divide in technology - What is it? What do we know about it?

3. Have participants to share their own stories of strength and resistance with technology? You can start out by asking the group - What is technology for you? Is it a good thing or a bad thing? Then, as an example, share your own personal story or anecdote about technology - this may encourage participants to be more open and comfortable speaking.

4. Once everybody who wants to share has had the chance to do so, bring out the pictures and corresponding bios of the women in tech that that you'll be introducing to the group. Arrange the photos and bios on a table or on the floor in no particular order, and then ask the group - Who do you think started first in the tech world?

5. Using the clothespins/alligator clips to affix the photos to the length of cord, have the group work together to arrange the women in chronological order to create a timeline of technological her-story; for example, they could be ordered by year of birth, or by year of their first major achievement in the tech field – just make sure that the group has access to that information so they can complete the exercise!

6. When the group is finished, they should then walkthrough and explain their timeline – ask them to share how many of the women and herstories they were already familiar with, and which ones were brand

new to them. The timeline of her-stories should remain hung in a visible place in the training room throughout the course of the workshop – to close the session, you can have the group take a few quiet minutes to read about each of these incredible women and their her-stories.

Optional: Since the her-story timeline will be visible throughout the training for the participants, another way you can lead this exercise is by closing it once the group has done the walkthrough of their ordered timeline. Once everybody is seated, you can share the bio of the first woman on the timeline and talk about why her her-story is important.

At the beginning of each following training day (depending on how many days and how many participants) have 1-2 participants do the same with the next 1-2 women in the timeline - that way, by the end of the training, every participant will have had the chance to contribute to the training by leading a mini-session, and you will have shared the stories of all the women in the timeline.

References

- https://donestech.net/lelacoders
- https://donestech.net/files/lelacoders_mujeres_programadoras_y_mujeres_hackers_es.pdf