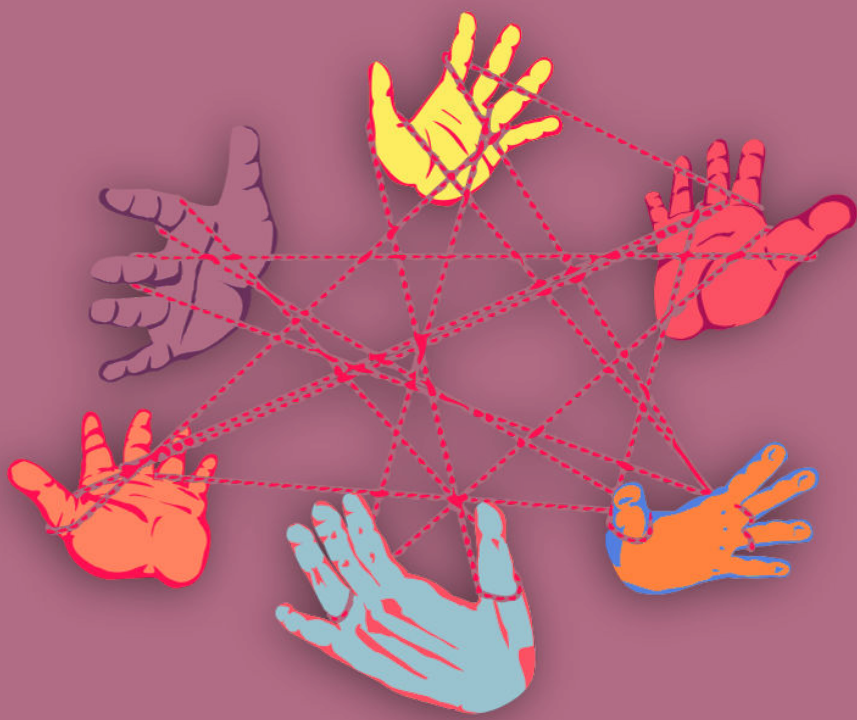




CYBERWOMEN



**Rethinking our
relationship with
technology**

Personal perceptions of security

**INSTITUTE FOR
WAR & PEACE REPORTING**



© 2019– Institute For War And Peace Reporting

<https://iwpr.net/>



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) license.

<https://creativecommons.org/licenses/by-sa/4.0/deed.en>

Contents

1 Personal perceptions of security	5
Leading the session	6
Part 1 - What is Safety for You? What is Security for You?	6
Part 2 - What Does Digital Security Mean to You?	8
Part 3 - Identifying Motivations, Resistances and Barriers	8
Part 4 – Digital Security, Gender and Technology Myths	9
Part 5 – Closing Affirmations	12
References	13

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 technology²

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 model³
- **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

Digital security



Physical security

Self-care

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>