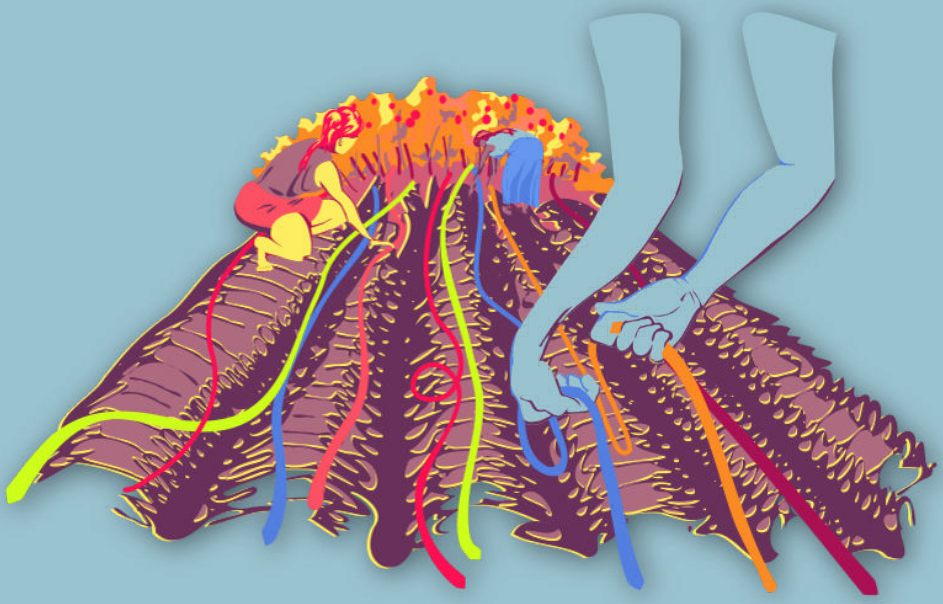
CYBERWOMEN



# Determining the best solution

# Determining the best solution




https://iwpr.net/

# Contents

# Gender-based risk model

- **Objective(s):** To lead participants through a process of first identifying the specific risks they face, both as women and as human rights defenders, and then designing an individual security strategy that addresses these risks.
- **Length:** 40-50 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - Various (see Recommendations below)
- **Related sessions/exercises:**
  - [Let's start a documentation journal!][]
  - Organizational security plans and protocols[1]
- **Needed materials:**
  - Pens and pencils
  - Colored Markers
  - Flipcharts or whiteboard/blackboard
- **Recommendations:** This session can be delivered a few different ways: (a)cover the entire session at the beginning of the training, with part

[1] https://cyber-women.com/en/planning-ahead/organizational-security-plans-and-protocols/

3 towards the end after you've covered more specific tools and practices in earlier sessions; (b)lead participants through parts 1 & 2 of the session near the beginning of your training, and then deliver part 3 towards the end after you've covered more specific tools and practices in earlier sessions; (c) split the session into 3 individual mini-sessions with part 1 near the beginning of your training, part 2 around the midpoint once participants have had the chance to discuss digital security in their personal contexts, and part 3 towards the end after you've covered more specific tools and practices in earlier sessions; (d) this session can be applied to both personal or organizational contexts, which is useful if a training is working with members of one collective or organization of whrds. this session involves a detailed discussion of personal risks through the lens of a women human rights defender context - especially by part 3 (in particular if this session is done all once, and not split into separate parts) it is likely that participants may begin to appear concerned or stressed. therefore, it becomes extremely important for you as the trainer to manage the level of stress in the room. make sure that at frequent intervals you remind the group that this session is ultimately focused on identifying strategies, tools, networks or allies that can help them to face risks; you don't want them to be or feel scared, there are lots of actions that they can take to fight online violence.

This session was prepared based on a session developed by Jennifer Schulte at IWPR's April 2016 Gender Retreat in Berlin, Germany, in consultation with the "Manual de Gestión del Riesgo de Desastre para Comunicadores Sociales" (UNESCO)

## Leading the exercise

### Part 1 – Identifying Risks & Probabilities

1. Start the session with a group discussion about the specific risks that women human rights defenders have faced, or can potentially face – remind the group exactly what is meant by the word "risk": the possibility of something happening which could cause damage or injury. Write down some of the specific examples of risks shared by participants – review these once you have an adequate number of them written down.
2. Turn the discussion towards the dynamic nature of risk – the probability of a risk occurring fluctuates depending on a number of external factors, increasing and decreasing in likelihood as these factors become more or less present – for example:
    - The risk of a text message being intercepted by an adversary increases when using a regular SMS app, but decreases if it is sent encrypted over an app like Signal;
    - Likewise, if someone is a targeted activist in their country, the risk of that text being intercepted is greatly increased if it is sent over a regular SMS app on a phone that is connected to their country's cellular network, but greatly decreased if sent using an app like Signal while on a cellular network in a foreign country;

    The above is a simple example of how external technical factors can impact the likelihood of a risk – but what about gender as a factor of risk? Are the risks faced by women human rights defenders the same as those faced by human rights defenders who don't identify as women?
3. Draw a table like the one below on a large piece of flipchart paper, and list out a number of digital risks under the "Digital Risk" column, using the different risks discussed and shared in Step 1 as examples (be sure to leave room on the right side to add additional columns for later parts of this session):

| Digital risk | Probability |
|---|---|
| | |

4. Once you've finished the above list, you will now work together with participants to identify for each risk the probability that it could become a reality – this is easier to do if your participants all come from a similar, shared context (country, type of activism, etc.); if there is a very wide variance among participants' backgrounds, you might want to offer a hypothetical "persona" as a working example for this part of the session.

5. To measure these risks' probabilities, you can formulate a scale. For example, you could use a simple scale of 1 to 5, where 5 equates to a "Very High" probability that the risk could become real and 1 is a "Very Low" probability.

   Which number can be assigned to each risk? You can start to fill the table out for the group as you discuss each risk individually, so it begins to look something like this:

**Probability (P):** 1 = Very low; 5 = Very high

| Digital risk | P |
|---|---|
| Accidentally clicking an email link with malware! | 4 |
| Our offices are raided by the police to seize hard drives or other devices! | 2 |

## Part 2 – Determining Impacts

6. Now that you have worked with participants to identify example risks and have established a simple system for assigning probability to each, explain that you will now move on to the next step – determining the actual impacts of these risks, or what the outcome would be to an indi-

vidual, organization, network, etc. if a given risk were to become reality.

7. Explain that, like the risks themselves, impacts are also quite dynamic – the exact nature of an impact and its severity are similarly contingent upon a number of external factors. Would the impact have implications on a personal level, or an organizational level? Maybe it has implications on both, and if so, how similar or different are those respective impacts?

8. For this next part of the session, you will be creating a scale to measure impact – this can be another quantitative (numerical) scale similar to the one that was used to measure probability, or it can be qualitative (descriptive) scale that describes the precise nature and detail of an impact. The choice is up to you and the participants – what is important is that this session highlight specific risks and outcomes in a way that facilitates participants' understanding of these as more than just abstract concepts (for the purposes of this session, we will use a quantitative scale).

9. Explain to the group that an important part of understanding and measuring a risk is to also anticipate how one might react to its impact - ask participants about how they would likely react on a personal level to a certain risk? Then, discuss how - as with probability and impact - you will also create a scale to measure reaction which can also be qualitative or quantitative (however, again, for the purposes of this session we will use a quantitative scale).

   Building off what you started to demonstrate in Step 5, your table should now look like the below example:

**Probability (P):** 1 = Very low; 5 = Very high / **Impact (I):** 1 = Low severity; 5 = High severity **Reaction (R):** 1 = Calm, under control; 5 = Panicked, highly stressful

| **Digital risk:** | P | I | R |
|---|---|---|---|
| Accidentally clicking an email link with malware! | 4 | 3 | 3 |

| **Digital risk:** | P | I | R |
|---|---|---|---|
| Our offices are raided by the police to seize hard drives or other devices! | 2 | 5 | 5 |

## Part 3 – Strategizing Solutions

10. As was mentioned in the Recommendations, this session involves a detailed discussion of personal risks through the lens of a women human rights defender context - it is likely that participants may begin to appear concerned or stressed by this point. Remind participants that this next part of the session will focus on identifying strategies, tools, networks or allies that can help them to face risks; you don't want them to be or feel scared, there are lots of actions that they can take to fight online violence.

11. Now that a probability, impact and reaction has been identified and measured for each risk, explain that this part of the session will address solutions. For each risk, ask participants: What can you do to address a risk and/or prevent it from happening? The answers given by the group are going to be different depending on at which point in the training process you are delivering this session – if it is closer to the beginning, they may not have very detailed answers, but if it's closer to the end of a training the responses they provide may be much more specifically related to certain practices or tools.

12. Going back to the table you've been working on over the course of the session, make a final column called "What Can I Do?" – under that column, write the answers shared by the group during Step 11. Once complete, keep the table posted visibly in the training room throughout the rest of the workshop so that participants can re-read and analyze their answers. This can help participants determine if anything additional should be added to the table, which can serve as a solid base for designing a digital security protocol.

    Below is what the final table should look like:

**Probability (P):** 1 = Very low; 5 = Very high / **Impact (I):** 1 = Low severity; 5 = High severity **Reaction (R):** 1 = Calm, under control; 5 = Panicked, highly stressful

| Digital risk | P | I | R | What can I do? |
|---|---|---|---|---|
| Accidentally [...] | 4 | 3 | 3 | Download and install antivirus software; warn others in my network/organization in case they encounter the same link |
| Our offices [...] | 2 | 5 | 5 | Make regular backups of our data, store them in a secure location outside the office, warn others in our networks if any of their information might have been compromised |

## References

- https://ssd.eff.org/en/module/assessing-your-risks

# 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/

# I decide

- **Objective(s):** To lead participants through a strategic critical thinking process to make decisions about specific digital security tools or practices that they will implement for themselves.
- **Length:** 15 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - Hands-on practice with digital security tools and practices from previous training
  - Digital security decisions[1]
- **Related sessions/exercises:**
  - Personal perceptions of security[2]
  - Who do you trust?[3]
  - How does the internet work?[4]

[1] https://cyber-women.com/en/determining-the-best-solution/digital-security-decisions/

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

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

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

  - Apps and online platforms: friend or foe?[5]
  - Digital security decisions[6]
- **Needed materials:**
  - Digital Safety Tool Figures (ideally 2-3 copies of each, but not enough to have one of each for every participant)
- **Recommendations:** As trainers, we can often impose our own vision of digital security practice on participants, either deliberately but with sincere intentions or unwittingly. however, it is important for us to remember that – as trainers and experts – our participants are under no obligation to either use the tools we teach, or to adapt to the practices that we deem to be "the safest".

## Leading the exercise

1. Open the session by explaining how building a digital security practice is a process that is iterative, and frequently difficult, for anybody. This session builds on the work started during the Digital Security Decisions session in this module, during which participants began to reflect on and identify their needs. Now, you will work with participants to begin identifying specific tools and practices for themselves.
2. On a table or other flat surface – this should in the middle of the training room, or someplace central and visible to all participants - place the digital safety tool figures (you will find the figures.
3. Tell participants that they will likely recognize many tools they have seen so far among the figured on the table - such as PGP keys, Signal, ObscuraCam or HTTPS Everywhere. Remind the group that, as has been mentioned previously throughout the training, it is they - not you as a trainer, not a technician, nor anyone else - who should choose the tools that best suit them and their needs.

[5] https://cyber-women.com/en/privacy/apps-and-online-platforms-friend-or-foe/
[6] https://cyber-women.com/en/determining-the-best-solution/digital-security-decisions/

4. Ask participants to come forward to the table, to select from among the tool figures on the table those which they think are important to them and their individual needs, and that they plan to continue practicing and using after the training process has completed.
5. Once everybody has chosen their tools, ask each woman to explain why they chose the tools that they did – they should stand or sit in a circle around the table, and go one by one until everyone has had the chance to share. They should also mention if there were any tools that they wanted to choose, but weren't able to because others had chosen it first.
6. Now, ask them if they think that there are any other tools missing from the table - even if they don't know the name of it (or even if it exists or not) ask them to say if they have any concerns remaining which are not readily addressed by any of the tools that were available to them.
7. Close the session with a group reflection about how knowledge is shared, and that those who chose a tool that other participants may have also wanted (but couldn't because there were not enough) should share and exchange it with them so that we can all "learn" from one another.