Cyberwomen

Contents

Part I

Introduction

Introduction to Cyberwomen

Within the last few years, various efforts have been undertaken to create improved resources, methodologies and practices for digital security trainings; however, very few of the resulting outputs have incorporated a strongly developed gender perspective. More recently, thanks to efforts within women's and feminist movements worldwide, a body of gender focused digital security content has begun to emerge – however, there remains a lack of coordination within the digital security community to grow this collection of resources in a strategic, responsive manner.

To that end, the Institute for War and Peace Reporting (IWPR) built the Cyberwomen curriculum with the intention of reflecting the rich technique and practice developed by women human rights defenders (WHRDs) leading digital security training efforts in the Latin America and Caribbean (LAC) region. Based on the experience of working with these women, we have created original training content with the aim of presenting a collaboratively-developed approach for training WHRDs on digital security from a holistic, gender-based perspective.

To avoid duplication of efforts, where we identified existing training materials already responsive to the needs of WHRDs – for example, those found within the LevelUp curriculum, or developed by organizations like Tactical Technology Collective (TTC) and Association for Progressive Communications (APC) - such content was incorporated directly into the curriculum and cited accordingly. However, the core value-add of

this resource lies in originally-produced modules and recommendations designed to offer learning experiences specifically tailored to the context of WHRDs working in high-risk environments.

Using the Cyberwomen Curriculum

This curriculum was designed with two specific user-profiles in mind: women trainers seeking to deliver gender-focused digital security trainings to women's groups, and members of these women's groups who, after receiving such training, now seek to pass that digital security knowledge onward to their own networks of colleagues and activists. In truth, not all sessions may be relevant to all audiences, and we encourage you to identify which sessions are most valuable for your specific audience and focus exclusively on those.

Cyberwomen includes interactive games, as well as audio-visual and graphic materials, as instructional aids for trainers; furthermore, its modules can be used either as stand-alone sessions or as components of a full training workshop. This modular structure allows trainers to select specific session content to match the needs of training participants; alternatively, trainers may also choose to follow suggested sequences of modules. From start to finish, to cover the entire curriculum would require approximately ten full days; for those trainers who wish to provide such a training, we strongly recommend separating delivery out into a series of workshops spaced over a period of at least six months. This approach will allow participating women the time required to effectively integrate new techniques and tools into their personal digital security practice, before moving on to acquire new skills.

Furthermore, as part of its focus on holistic security, the curriculum incorporates specific content on feminist self-care and recognizing gender-based violence, whether symbolic or online. The objective of these sessions is to reinforce participants' sense of agency and control over their safety and identities – therefore, it is important that they be integrated throughout trainings as spaces for individual and collective action and reflection, rather than covered as a standalone module by themselves.

Finally, there are many exercises included in this curriculum - some

are trust-building exercises, which should be done at the beginning of the first training day; others are basic icebreaker exercises, which can be done at the beginning of any training day. Finally, there are several exercises designed to reinforce specific training content which should only be done in their listed order. The curriculum also includes resources for follow-up sessions to be delivered over the suggested period of six months.

A Feminist Approach to Curriculum Development

As mentioned previously, this curriculum integrates a holistic vision of security for WHRDs, including the "Triad" of digital security, physical security and self-care; however, the core of the training is focused on digital security. To integrate a more gender-sensitive, feminist approach, this curriculum was produced with the following core values and principles in mind - we strongly encourage trainers to take these into account while planning workshops using this curriculum:

Women Participants and Women Trainers

First and foremost, Cyberwomen content is designed to support an ambiance of woman-to-woman confidence and trust in a training setting. Participants in digital security trainings frequently come from places – both physical and emotional – of high stress or anxiety; women human rights defenders are also frequently the targets of harassment and violence both online and offline. It is paramount that women participants perceive a training as a safe space, where they can feel at ease sharing their fears, doubts and emotions, and can actively participate and engage with others; therefore, this curriculum is intended for women trainers working with women participants. However, we also encourage male trainers to review this curriculum and its foundational principles to better adapt their own training practice to working with mixed groups in a workshop setting.

Female and Feminist Models

This curriculum was created with a focus on sharing real-life instances of digital attacks - as experienced by women human rights defenders,

activists and journalists - using empowering testimonies. Recognizing that not every woman at a given workshop will define herself as a feminist, the curriculum's approach to the training process focuses on raising awareness about online violence against WHRDs, first by highlighting differences between attacks on male and female activists, and then by providing examples of online gender-based violence (e.g. on social media platforms) as a means towards helping women identify the violence they may already be facing in these spaces. As part of this methodology, we presented case studies that were close to the women's everyday life, making it easier for participants to relate to different situations and thus understand the relevance to their own context. We found that using this approach empowered participating women to more consistently practice new skills and subsequently provide digital security advice to others.

My Body, My Devices, My Decision!

The central ideas, information and practices shared in this curriculum are grounded in promoting digital autonomy. Central to the design of this curriculum is an emphasis on "strategic thinking about digital security" - sharing digital security concepts with participants, rather than just training on a list of tools. A great deal of time is dedicated to introducing participants to digital security concepts such as encryption, anonymity, privacy and open-source software before training on related tools. By empowering women to develop a personalized understanding of these concepts, they come away equipped with the information they need to make their own decisions about which tools are best for them.

Analysis of Gender-Based Risk and Social Media

By using examples from YouTube videos, messages on various social media platforms, and outputs emerging from other training sessions, this curriculum aims to hold a safer space for discussion and reflection on technology-based violence that specifically targets women. Specifically, much of this comes together in the Online Violence Against Women module; likewise, the Gender-Based Risk Model exercise found in the module Determining the Best Solution is focused on sharing experiences

and identifying vulnerabilities participants face not only as women but as human rights defenders (in this case, in the LAC region).

Feminist Self-Care & Digital Self-Defense

As part of a holistic approach to security, this curriculum considers emotional well-being and self-care as a vital element of security for WHRDs; likewise, as part of a focus on digital autonomy, there are specific sessions – the session Gender-Based Risk Model again serving as an example – which are intended to help participants prepare for and react to digital attacks. This curriculum is an effort to provide information for participants to identify and explore several strategies for their digital self-defense; these include, but are not limited to, separating the personal from the public, creating online identities, 'doxxing the troll', encrypting their communications, and documenting digital incidents. By equipping participants with a better understanding of their online environment – across both the platforms they use and the risks associated with each – we can empower them to develop strong digital security habits that can in turn become part of a holistic practice of self-care.

Planning resources

- **Objective(s):** Pre-training assesment and evaluation

Pre-Training Assessments

Crucial to the training planning process is gathering the data points needed to design a training agenda. A solid understanding of participants' digital security needs often means the difference between an effective training responsive to participants' goals and context, and an ineffective training potentially exposing participants to greater risk than they were previously.

Knowledge of how potential participants use technology, how they communicate with it, and what prior digital security knowledge they may possess will have a significant impact on the scope of content to be covered.

Assessing Needs and Motivations

Ideally, you will be able to carry out a needs assessment ahead of your training, by working either with the training participants themselves or with a member of their representing organization. Bear in mind that beyond objectively assessing their needs, it will be important to also understand their

motivations for participating in a training – are participants proactively seeking to boost their own resilience, or are they requesting assistance in response to recent or ongoing incidents? Furthermore, from a practical standpoint, knowing how much time you have available ultimately determines how much content you can cover in a single workshop (or subsequent ones); this is furthermore determined by the collective skill level of the participants.

If you have the opportunity for in-depth interaction and communication with participants before your training, below are some questions to ask that can help you learn more about them and/or the organization they work with:

- What is their organization's background?
- How is their organization's team configured?
- What are their organization's main programs and/or activities?
- What are some of their technology-related practices? How and from where from do they access the internet?
- Which type(s) of computers and/or mobile devices do they use? Do they have separate devices for work and personal use?
- Which operating system(s) do they use?
- What other movements or groups do they collaborate with? This can be as a representative of their organization (e.g. as coalition members) or personally as independent activists.
- Have they ever experienced any incidents or direct threats to their physical or digital security? This could be related to their devices, equipment, online accounts or physical aggression.

Digital Security and Capacity (DISC) Tool

If there is the opportunity to engage in a comprehensive assessment process with training participants in the time leading up to your workshop, included in this curriculum is the DISC (Digital Security and Capacity) Tool,

a resource which IWPR has produced and used extensively for assessment processes ahead of digital security trainings.

The DISC Tool is a pre-training assessment questionnaire that uses a quantifiable scoring mechanism to gauge participants' existing digital security skill level, while also providing qualitative information on strengths and areas for improvement at a more granular, practice-specific level. If you will be working with participants on an iterative basis (for example, leading several trainings over a 6-month period), DISC Tool is also a useful way to track their learning and comprehension progress.

The full DISC Tool resource can be found here[1]

Alternative Assessment Strategies

In the event that you're not able to perform a pre-training assessment directly, or have these questions answered, you can still infer quite a bit of background information from what you do know about participants' context and circumstances:

For instance, if you're aware of women activists or organizations conducting similar work in the same region as the group(s) you will be working with, it is likely that any risks or attacks they have faced will be similar in nature to those that your participants might have encountered.

Furthermore, there may be certain known threats or incidents that you can correlate to the kind of work that your participants do (and where they do it). If you will be training women lawyers providing legal counsel to other WHRDs, or women journalists reporting on government corruption, you may be able to research some of the tactics that governments or other non-state actors in their country have used in the past against individuals, in particular women, doing similar work.

Example training agendas

Although we are aware that the final content of a training session will be based on the diagnosis each trainer does of the group the will work with

[1] https://cyber-women.com/en/DISC/

and we invite each trainer to adjust this session to better meeting the needs of the group, we do suggest a few options for what we think could be regular scenarios of trainings.

The example agendas below are organized by length (in days), and then by participant skill level. Other planning parameters will of course inform the ultimate design of your training; however, time is almost always the most critical:

How much time you have available ultimately determines how much content you can cover in a single workshop; this is furthermore determined by the collective skill level of the participants.

You're more likely to know how many hours or days are available to work with a group before knowing other factors, such as the venue, the number of participants, or their collective skill level.

Read more[2]

Although we are aware that the final content of a training session will be based on the diagnosis each trainer does of the group the will work with and we invite each trainer to adjust this session to better meeting the needs of the group, we do suggest a few options for what we think could be regular scenarios of trainings.

The example agendas below are organized by length (in days), and then by participant skill level. Other planning parameters will of course inform the ultimate design of your training; however, time is almost always the most critical:

How much time you have available ultimately determines how much content you can cover in a single workshop; this is furthermore determined by the collective skill level of the participants.

You're more likely to know how many hours or days are available to work with a group before knowing other factors, such as the venue, the number of participants, or their collective skill level.

[2]https://cyber-women.com/en/agendas/

Acknowledgments

Some sessions and other information adapted for this curriculum were developed by: Association for Progressive Communications, Tactical Technology Collective, Fundación Karisma, Mujeres Al Borde, Elis Monroy from Subversiones Collective, Danah Boyd, Mariel García, Alix Dunn, Spyros Monastiriotis and Phi Requiem.

- **Authors:** Alma Ugarte Pérez, Indira Cornelio Vidal and Dhaniella Falk
- **Coordination and Systematization:** Alma Ugarte Pérez, Indira Cornelio Vidal and Dhaniella Falk
- **Education and Localization:** Nicholas Sera-Leyva
- **Spanish translation:** Nadège Lucas Pérez
- **Coordination of Peer-to-Peer Learning and Session Pilots:** Estrella Soria
- **Consultancy:** Tierra Común cooperative[1]
- **Web development, graphic design and media production:** Kéfir cooperative[2]
- **Peer Reviewers and Collaborators:** Azza Sultan, Carol Waters, Dalia Othman de Tactical Technology Collective, Estrella Soria, Erika Smith from the Association of Progressive Communications, Gigi Alford, Jennifer Schulte, Laura Cunningham, Lindsey Andersen,

[1] https://tierracomun.org
[2] https://kefir.red

Megan DeBlois from Internews and Sandra Ordoñez.

Part II

Trust-building exercises

The rules of the game

- **Objective(s):** Collectively build shared participation and co-existence agreements for your training - “the rules of the game”. – together with participants.
- **Length:** 8-10 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Tricky candy[1]
  - Defenders bingo[2]
- **Needed materials:**
  - Flipchart paper (or blackboard/whiteboard)
  - Markers
  - Colored stickers (3 colors – red/pink, yellow and green ideally)
- **Recommendations:** Part 2 of this exercise – “traffic light” - works best if participants have nametags for themselves onto which they can put their colored stickers (see instructions).

[1] https://cyber-women.com/en/trust-building-exercises/tricky-candy/
[2] https://cyber-women.com/en/trust-building-exercises/defenders-bingo/

Leading the Exercise

For any training process, although there is usually already an established relationship of some kind both among participants and with you as the trainer, it is essential to establish mutually agreed upon coexistence agreements (which we'll call "the rules of the game) that support a pleasant and respectful environment for all involved.

Every woman's lived experience and cultural context is unique, and something which may seem completely inoffensive to one could be interpreted differently by others. Collaboratively developed coexistence agreements help ensure that a training holds space for these different perspectives and personal comfort zones; for instance, some women may feel uncomfortable about physical contact, while others may use physical contact as a way of expressing themselves. As another example, consider even that some participants with a more traditional educational background may feel the need to ask permission to use the bathroom, while for others it may be totally normal to simply leave the room.

This session will help you generate these collective coexistence agreements, in recognition of participant preferences that will allow them to feel comfortable – and thus more receptive to learning - throughout the workshop.

Part 1 – The Rules of the Game

1. Briefly explain the above background to participants, and then ask them for examples of coexistence agreements that they feel are important and essential to their comfort during the workshop. You can start off with an example of your own – this could be something like "we do not need permission to go to the bathroom" or "we will not share anything about this training on social media without permission".
2. On flipchart paper or a blackboard/whiteboard, write each agreement shared by the group as they are spoken. Once you feel that there are enough, reach each agreement out loud - ask participants if these appear to be good rules of coexistence for the group. Unless

this has already been mentioned - or you offered this as a starter example agreement - it may be helpful to also bring up agreements about the use of laptops and phones during sessions.

3. Remind the group that these agreements will remain posted and visible for the duration of the training, and that they can be modified at any time upon discussion and agreement of the entire group. Be sure to also offer participants the option of making suggestions directly to you or anonymously, in case they don't feel comfortable doing so openly.

Part 2 – "Traffic light"

4. There may be certain agreements on your list for which there are varying levels of comfort within the group. For these agreements, such as those related to physical contact or photography, you may want to offer participants a way to indicate their own comfort level to one another.

5. Distribute the colored stickers to each participant, making sure to give them several of each color. Explain that for some of the coexistence agreements on the list, the group will be doing a mini-exercise called "Traffic Light" (indicate which agreements you are referring to).

6. Using the example of an agreement about physical contact which reads "Before making any physical contact with another participant, we will make sure that they are comfortable with it first" or similar, the group should assign a meaning to each colored sticker as it related to that agreement – for instance:

Red/Pink: "Physical contact bothers me a bit, please respect my space." **Yellow:** "I don't mind physical contact but please ask first." **Green:** "I don't mind physical contact at all"

7. Participants should then choose a colored sticker for themselves based on which of the agreed upon definitions matches their personal comfort level, and place it on their name tag. You don't need

to have each participant share which color they selected, as everyone should be able to see which colors others have chosen.

8. Write the definitions and colors on a new sheet of flipchart paper for each rule that this will apply to - it shouldn't be more than 2 or 3. If there will be 2 or more, have participants write an identifying letter on each (for example, "C" for "Contact" or "P" for "Photos").

Defenders bingo

- **Objective(s):** You and your participants will begin introducing yourselves to one another in this icebreaker exercise, which is built around an interactive game that encourages participants to get to know each other beyond just names.
- **Length:** 12-15 minutes depending on group size)
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Tricky candy[1]
- **Needed materials:**
  - Bingo sheets for each participant (pre-filled with participants' names)
  - Blank index cards
  - Pens/pencils (enough for all participants)
  - Optional: Markers and blank sticky labels (for name tags)

[1] https://cyber-women.com/en/trust-building-exercises/tricky-candy/

Leading the Exercise

Remembering names and identifying faces is more difficult for some people than it is for others. This "icebreaking" exercise will help participants remember these details while also allowing them to learn more about the people they will be working with throughout the training process – each other!

1. Have each participant write their first name on a blank index card, and collect them all once everybody has finished.
2. Next, give everyone a Bingo sheet that's been pre-prepared with all participants' names (see example below) – optionally, you may also include your name on the board.

   Example of a pre-prepared Bingo sheet:

Alma	Kim	Sophie
Heidi	Cristina	Roua
Marcela	Tippy	Indira
Anaiz	Lulu	Maria

3. Explain to the group how the game works:
   - You will read aloud, one by one, the index cards that participants filled in with their names;
   - As you read out names, participants will circle each name where it appears on their Bingo sheets;
   - The first participant to circle a complete row of names (horizontally or vertically) will shout "Bingo!" and be declared the winner.
4. Ask the winner to read aloud the name of the first participant in their winning row – the person named will stand up, repeat her name, and

then add a detail (choose which ahead of time and let them know as part of your instructions) such as what she likes to do in her spare time, what her favorite movie or song is, her favorite food, etc.

5. The winner will repeat the process in Step 4 until each participant in their winning row has introduced themselves. As each name is called, take its matching index card from the stack you used in Step 3 and set it aside.

6. Once the winner has finished calling out the names in their winning row, thank them; then, read aloud the names on your remaining index cards so that each participant has the chance to introduce themselves to the group.

7. Once all the participants have introduced themselves, it's your turn! Repeat your name for the group and share a detail about yourself as well. Close the exercise by reminding the group that you are all starting a new adventure together, and that knowing and recognizing each person in the group will be very important to the success of your journey.

   Optional: At the end of the exercise, give each participant a blank sticky label and a marker so they can make their own name tag – this not only helps participants remember each other's names, but also helps you to do the same (always a plus for your training process!)

Tricky candy

- **Objective(s):** You and your participants will begin introducing yourselves to one another in this icebreaker exercise, which is built around an interactive game that encourages participants to get to know each other beyond just names.
- **Length:** 5 to 8 minutes (depends on group size)
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - The rules of the game[1]
- **Needed materials:**
  - 1 or 2 bags of fun-size candy
  - Optional: multiple varieties of candy, or candy in several different colored wrappers

Leading the Exercise

1. Offer candy to everyone in the group, telling them to take as much as they'd like. Some participants will take more, others less, etc. You

[1] https://cyber-women.com/en/trust-building-exercises/the-rules-of-the-game/

can also take some for yourself.

2. Once everyone has taken some of the candy, reveal the "trick" to everyone – for each piece of candy they took, they must share with the group a personal quality or interesting detail about themselves. These could include things like:

- A wish or a personal goal
- A something they enjoy about their work
- A country or place they'd like to visit

Optional: If you have multiple varieties of candy, or candy in several different colored wrappers, you can assign a specific category to each variety or color. Using colored wrappers as an example, you could do the following: * Red wrapper = a wish or a personal goal * Green wrapper = something they enjoy about their work * Blue wrapper = a country or place they'd like to visit

Who do you trust?

- **Objective(s):** Lead participants through a process of reflection with the goal of identifying perceived allies and adversaries in each of their individual contexts. the allies and adversaries identified in this quick exercise will help you facilitate a training that is more relevant to your participants, as you will be able to better contextualize different sessions to their specific context(s).
- **Length:** 15 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Organizational security plans and protocols[1]
  - Digital security plans and protocols: post-training replication[2]
  - Gender-based risk model[3]
- **Needed materials:**
  - Several large sheets of flipchart paper

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

[2]https://cyber-women.com/en/planning-ahead/digital-security-plans-and-protocols-post-training-replication/

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

Leading the exercise

1. Give each participant one sheet of flipchart paper; then, give the group the following prompt as a contextualizing introduction to the exercise:

   > Nobody trusts everyone, but nobody doesn't trust anyone

2. Give everybody 5 minutes to answer the following questions individually; as they do so, also ask them to identify for each whether their response might change when answered in a personal context versus when answered in a work/activism context:

   - Who do you trust?
   - With whom do you think you could trust your information?
   - With whom do you think you could not trust your information?
   - Who do you think could be spying on you?
   - Who is not spying on you?

   Examples of people or adversaries that may come up in response are government actors (e.g. state security), private companies (e.g. Facebook or Google), Internet Service Providers, close partners and friends, or even colleagues.

3. Once time is up, split participants up into groups of 3-4 people (maximum) to discuss their answers with each other – after 10 minutes have passed, each group should then share with the rest of the participants what they discussed.

4. Now, you can close out the exercise by explaining that over the course of this training – based on the adversaries the group has begun to identify in this exercise - you will be able to highlight practices and tools which are more relevant to their specific contexts.

Part III

Rethinking our relationship with technology

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]
  - Gender-based risk model[3]

[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/

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

- **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?

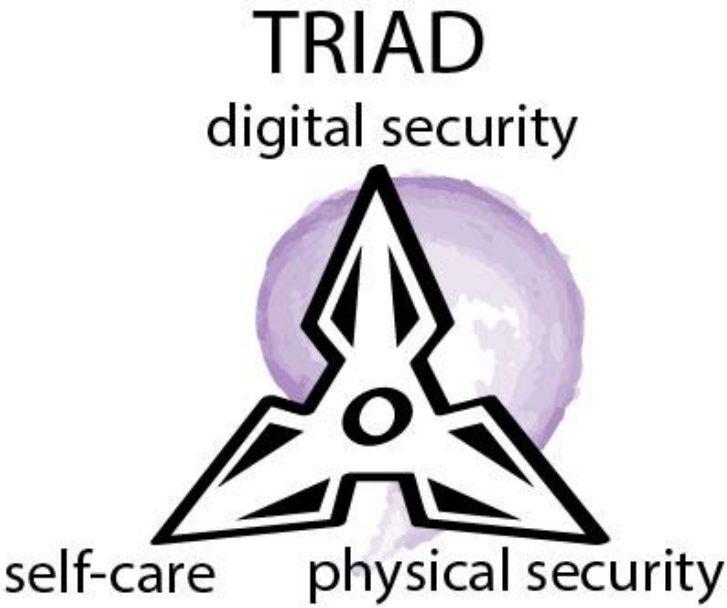
1. Ask participants split up into small groups of 3-4 people (maximum), giving them 15 minutes to discuss the following questions with each other:

- 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 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.



Holistic security triad

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. 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' [1]:

> 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]
  - Privacy[5]
  - How does the internet work?[6]

[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/

[5] https://cyber-women.com/en/privacy/privacy/

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

  - 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 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

[7] https://cyber-women.com/en/online-violence-against-women/a-feminist-internet/

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 her-stories 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

Part IV

Digital security basics 1

How does the internet work?

- **Objective(s):** Csharing an understanding the flow of information across the internet, and the different vulnerabilities and related good security practices at each point of the chain.
- **Length:** 60 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Who do you trust?[1]
  - Personal perceptions of security[2]
  - Your rights, your technology[3]
- **Needed materials:**
  - How Does the Internet Work? placards – these should be iconic representations of the parts of the chain that an email goes through when it is sent from one computer to another: devices (computer/mobile phone) (x 2) (it's best for the computer and the phone to be on the same piece to avoid

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

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

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

confusion.), modem (x2), telephone pole/underground optic fiber (x 2), internet service provider (x 2), Google servers (x 1), mock email (x 2, o más)
  - Handouts with suggestions of digital security practices
  - Paper to use as a board – one long piece (4 meters), and two smaller pieces (1 meter)
  - Colored markers
  - Adhesive tape
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
  - Speakers
- **Recommendations:** Make sure to cover all the questions participants might have. it is important they leave the session with answers to their concerns with the vulnerabilities they learned about, and feeling they have the information they need to take action. avoid creating an environment of fear, stress or anxiety - provide enough information and resources, as well as further training opportunities (if possible)

This session was developed jointly by Mariel García (SocialTIC) and Spyros Monastiriotis (Tactical Technology Collective)

Leading the session

Part 1 - How the Internet Works – Flow of Information and Points of Vulnerability.

1. This part of the workshop will begin as a game. Participants will be given pieces of paper representing one part of the chain of the flow of information online (modem, computer, ISP building, etc) and will be asked to arrange themselves in the order they consider is correct to represent the way an email travels through the Internet to reach another computer.
2. Once the group is arranged, the facilitators will correct any mistakes, and will do a run-through explaining the process to everyone.

Then a volunteer will be asked to repeat that explanation. It is recommended that the complete explanation is made at least three times; but, to give variety to this exercise, the facilitator can change the email illustrations that are used, and the extreme where the demonstration begins. The trainer must also give some time to clarify doubts related to this process.

3. You can also use a video like this one https://www.youtube.com/watch?v=7_LPdttKXPc to help participants identify any mistakes that they have in the way they arranged themselves.

Optional: To adapt this for larger groups - rather than giving out one piece per person, assign one piece to a pair; for smaller groups, they can place the pieces on the floor, debating their order.

Part 2 - Vulnerabilities

4. When the previous process has been completed, participants will be asked to paste each piece on a long paper (from a roll) that will be left on the floor. At this point, the facilitators will go through the chain again, this time to point out and explain the vulnerabilities at each stage (and hint at good practices to keep participants calm and confident).

Some of the vulnerabilities are mentioned next. You can also add any other practice or threat that is applicable in your own context or that is relevant to mention to the participants. You can also share a few examples of practices that other collectives you work with have to help participants think of what might be some of their own good or bad practices.

Device 1 (computer/phone): Physical insecurity; loss of information

Modem 1: Wifi sniffing; lack of encryption

Telephone pole/optic fiber underground: N/A

Internet Service Provider: Data and metadata requests from local/national governments

Google Servers: International surveillance; password insecurity and phishing, requests from national governments

Telephone pole/optic fiber underground 2: N/A

Modem 2: Security problems using other people's connections (like at Internet cafes)

Device 2: Malicious software; insecure deletion

Part 3 - Good Practices for Digital Security

5. After focusing on vulnerabilities, it will be time to break the group into smaller ones that can "adopt" one of the vulnerabilities discussed in the previous exercise and propose creative solutions for it. To make it less overwhelming for less experienced participants, each group will be given a piece of paper including one solution proposal that can ignite conversation.

At the end, the groups will be given 30 seconds to a minute to present their ideas to the rest of the group (while one of the facilitators takes notes and makes additions to what is reported back by the groups). Facilitators will float around the groups giving brief explanations and answering questions, and mostly promoting discussion among all the participants.

It's important that, as this activity progresses, facilitators explain the basics of each solution. Also, depending on the level of interaction and speed of the workshop, it may not be possible to cover all the proposals.

References

- https://securityinabox.org
- https://myshadow.org

Building stronger passwords

- **Objective(s):** In this session, you will review with participants the implications of a compromised password, how they are commonly compromised, and how to create stronger passwords and develop better password habits.
- **Length:** 45 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - How does the internet work?[1]
  - How to secure your computer[2]
- **Needed materials:**
  - Projector
  - Slides
  - Paper
  - WiFi/internet access to download KeePass

This session is based on the module "Safer Password Practices" developed by Cheekay Cinco, Carol Waters and Megan DeBlois for LevelUp

[1] https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/
[2] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/

Leading the Session

Part 1 - Introduction

1. Start this session asking participants:

- When was the last time they changed any of their passwords?
- Do they have different passwords for their different accounts?
- Do they have their password written on a post-it note?
- Do they have all their passwords stored on a document?
- Do their phones have a password?

Part 2 - Why are Passwords Important?

2. Before you begin talking about the importance of passwords, ask participants to list all the information that is being kept safe through a password. What information do they have in their email accounts, social media accounts, cell phones? What would happen if someone else were able to access that information?

3. Now, share with the participants some reasons why passwords are important:

- Passwords provide access to a number of important accounts such as email, banking accounts, social networking sites, etc.
- These accounts often contain sensitive information, and also allow us to "be ourselves", permitting organic interaction with others using various digital services - this might entail sending a social networking message, sending an email, making an online purchase, etc.
- They may also allow us to appear to be others - anyone with access to an account password can, in effect, act online as if they were the account owner.
- Passwords also provide access to a number of other things - Wi-Fi access points, unlocking mobile devices, logging-in to computers, decrypting of devices, files and more

Part 3 - What Can Happen If Your Password is Compromised?

4. In this part of the session we will share the papers with the participants and ask them to list all the platforms they can remember they have an account on. Now ask participants to list what might happen if someone had their password and could accessed their accounts or devices:

- Important information or files could be stolen (copied) or deleted; if they are stolen, you may or may not realize it immediately. This could be anything from sensitive documents and files, to address book contacts and email messages.
- Money and other funds could be stolen or spent, via access to credit cards or bank accounts.
- Email or social media accounts could be used to send spam, or used to impersonate you or your friends, family, and colleagues.
- Account access could be held in exchange for a form of "ransom" - this could include money, access to contacts, or access to other accounts.
- Someone with a password could use this access to monitor communications and activities without your knowledge.
- Access to your email could set off a "domino effect" where it is used to reset passwords to other accounts by requesting password reset links, eventually locking you out of many other accounts if the password remains unchanged.

Part 4 - How are Passwords Commonly Compromised?

5. Share some of the common practices that can end up with other people having access to your passwords:

- When they are shared with others, or stored in an easily discoverable way - a commonly seen example is a computer login password written on a post-it note, and then stuck onto the same computer or nearby.

- When someone witnesses a password being entered on your screen and writes it down or remembers it.
- If using an email client without SSL (https) session-wide, only at the login page, this leaves passwords and other information vulnerable as they are visible by anyone with access to the connection after logging in.
- A device is physically accessed, and passwords are able to obtained through "Save My Password" or "Remember Me" settings saved on websites via a browser - this is especially possible if full-disk encryption isn't used on a device.
- Malware, such as a keylogger which can document every keystroke on a device and send it to a waiting third-party, can reveal not just passwords but potentially a great deal more personal or sensitive information.
- Platforms can also be hacked or vulnerabilities in their systems cause that their users information is exposed.

Part 5 - How Can We Make our Passwords Stronger?

6. Explain that if we use the same passwords for everything, and that password is compromised, all our accounts can be compromised. Share some qualities of safer, stronger passwords with the group:

Length: to put it simply – the longer, the better! 12 characters is a highly recommended minimum for strong passwords, and 20 characters is even better.

Complexity: use a password that's alpha-numeric, using upper and lower case letters, with a generous mix of numbers and special characters.

Changed Regularly: regularly change your passwords, particularly for your most sensitive accounts, and definitely change them if you receive an authenticated (not phishing) email telling you that a particular service has had user accounts and passwords compromised.

Using passphrases (imagine several passwords strung together into a "sentence" or phrase) is another example of a strong password practice –

here are a few examples:

> NoALaMineriaEnAmericaLatina ("Say no to mining in Latin America")
>
> AbortoSiAbortoNoEsoLoDecidoYo (Abortion yes, Abortion no, that's for me to decide)
>
> NosotrxsNoCruzamosFronterasEllasNosCruzanANosotrxs (We didn't cross borders, borders crossed us)

7. Ask participants to take a few minutes to begin creating some examples of strong passwords. Remind participants that they should think about how sensitive the information is in a given account while they consider the length or complexity of their passwords – they may want to use their strongest passwords for their most important accounts, while using less complex (but still strong!) passwords for less important accounts.

References

- https://level-up.cc/curriculum/protecting-data/creating-and-managing-strong-passwords/input/safer-password-practices/

Malware and viruses

- **Objective(s):** This session addresses the basics of what malware is, and how user devices can become exposed to different kinds of malware, in the context of risks most typically encountered by women human rights defenders.
- **Length:** 30 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - How does the internet work?[1]
  - How to secure your computer[2]
  - Let's reset![3]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
- **Recommendations:** Ideally, this session will be followed by the "how to secure your computer" session, which is also in this module.

[1] https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/
[2] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/
[3] https://cyber-women.com/en/digital-security-basics-2/lets-reset/

Leading the Session

Part 1 - Introduction to Malware

1. Explain to participants what malware is, and review a few of the types of malware that exist – at a minimum, it is recommended to cover the following:

- Trojan Horse
- Spyware
- Ransomware
- Keylogger

Ransomware and keyloggers are increasingly common types of malware encountered by women human rights defenders in Latin America; if you are working with a group of women from that region, these will be important to address. Likewise, in general, make sure to include case studies and examples of malware that are commonly encountered in the context of the participants attending your training.

Part 2 - How Can You Get Infected?

2. Explain some of the most common ways that devices become infected with malware, and the unsafe practices that can lead to such infections. It is also important to explain the different purposes or motivations behind malware deployments:

- Some malware is broadcast on a wide-scale with no particular target;
- Other kinds are specifically targeted at activists, journalists or dissidents to gain access to their data or communications;
- Still other kinds are targeted at individuals known to be connected to a number of activists, journalists or dissidents in the hope of infecting multiple targets across a network.

Part 3 - Share Examples Involving Women & Women Human Rights Defenders

3. Finish the session by sharing examples of malware infection scenarios typically encountered by women and WHRDs; you can also share specific case studies involving women and WHRDs (from blogs, news or personal experience – always anonymize these unless you have explicit permission from the target to share their name)

Here there are a few general examples of cases, and you might also know similar cases to these in your context as well:

- A woman who received an email about an opportunity to get free tickets for a concert; the link within the email infected her smartphone with malware.
- A woman activist that received a message from what appeared to be the email of a colleague; after clicking the link within the email, her computer hard drive "encrypted" and a message appeared on her screen requiring payment in order to regain access to her information.

Safe browsing

- **Objective(s):** Provide an introduction to safe web browsing practices, including an overview of plug-ins and other utilities that can be used to create a safer browsing environment.
- **Length:** 45 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - How does the internet work?[1]
  - How to secure your computer[2]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
  - WiFi connection

[1] https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/
[2] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/

Leading the Session

Part 1 - Choosing a Browser

1. Begin the session by asking participants which web browsers they use and what other options they have heard of. Present Firefox - explain the benefits of using it, and discuss briefly the difference between it and other common browsers such as Google Chrome or Internet Explorer.

   Optional: If working with Spanish speaking women, you might also find this video from Ella useful to begin the conversation: https://vimeo.com/109258771

Part 2 – Safer Browsing Practices

2. There are quite a few safer browsing practices to discuss that can be shared with participants – while you don't need to cover every single one of them, it is recommended to share enough to give your participants options (also remember to keep your content contextualized by sharing practices most relevant to participant context).

3. Explain to the group that you will be reviewing some safe browsing practices with them, but not yet focusing on specific tools other than the browsers themselves. Some participants might already be willing to change browsers, but others may not yet be – so before discussing more specific tools like browser plug-ins, it's important to keep the discussion grounded first in practice.

   Here are some example practices you can discuss:

   - Being vigilant of phishing and spear phishing attempts;
   - Blocking embedded ads and pop-up ads;
   - How cookies work – be sure to talk about how convenient they can be, but that they also have downsides;
   - Disabling and erasing cookies from the browsers;
   - Deleting browsing history;
   - Not saving passwords in your browser settings;

- Checking the extensions that you add to your browser;
- Enabling the Do Not Track option in your browser;
- Google search alternatives (such as Duck Duck Go)
- Who implements online tracking and why? (Both https://trackography.org and https://www.mozilla.org/es-MX/lightbeam/ are good resources about this);
- Discuss HTTP versus HTTPS;
- What is a VPN (Virtual Private Network) and when should these be used?
- What exactly does Incognito Mode do, and when should it be used?

Part 3 – Tools and Extensions for Safer Browsing

4. Explain, now that you've addressed some basic practices for safer browsing, that you can also suggest certain tools – specifically browser plug-ins – which can help automate or otherwise facilitate adoption of some of these practices.

5. Present the following tools, explaining how each of them works, and remember to also share the links to download them with participants. It is essential that participants understand why each of the tools shared is important and useful; if not explained clearly, it can lead to participants making ill-informed decisions about their privacy or anonymity online.

Desktop Browser Tools

- No Script[3]
- Adblock Plus[4]
- Privacidad Badger[5]
- HTTPS Everywhere[6]

[3] https://noscript.net
[4] https://adblockplus.org/
[5] https://www.eff.org/privacybadger
[6] https://www.eff.org/https-everywhere

- Click & Clean[7]
- Tor browser[8]
- Disconnect[9]
- uMatrix[10]

Mobile Browser Tools

- HTTPS Everywhere[11]
- Recursos de My Shadow[12]
- Orfox[13]
- Orbot[14]
- Tor for iPhone[15]

Other Practices & Features:

Incognito Mode (InPrivate Mode) This is a feature that frequently causes confusion as it is not well understood - participants might not have a clear understanding of how Incognito mode works as a browser feature, and when it is useful. Explain how Incognito (and similar) modes work, and offer some examples of when they can actually be helpful features to take advantage of.

Safe Wi-Fi Practices

Finally, take some time to discuss, and if possible demonstrate, a few basic safe practices on for WiFi connections - this includes practices such as changing the default password of the modem, and showing participants how to monitor which devices are connected to their WiFi network.

[7] https://www.hotcleaner.com
[8] https://www.torproject.org/download/download-easy.html.en
[9] https://disconnect.me
[10] https://addons.mozilla.org/es/firefox/addon/umatrix
[11] https://www.eff.org/https-everywhere
[12] https://mike.tig.as/onionbrowser
[13] https://mike.tig.as/onionbrowser
[14] https://mike.tig.as/onionbrowser
[15] https://mike.tig.as/onionbrowser

Referencia

- https://myshadow.org/es/trace-my-shadow
- https://securityinabox.org/es/guide/firefox/windows
- https://securityinabox.org/es/guide/firefox/linux
- https://myshadow.org/es/tracking-data-traces
- https://cuidatuinfo.org/article/firefox-y-complementos-de-seguridad

How to secure your computer

- **Objective(s):** Identifying good practices to keep our computers safe.
- **Length:** 50 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - How does the internet work?[1]
  - Safe browsing[2]
  - Malware and viruses[3]
  - Storage and encryption[4]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
  - Printed copies of the Backup Format Template (see below)
- **Recommendations:** It is strongly recommended that you do live demonstration – using a projector connected to your laptop - of any tools you choose to cover in this session, so that participants can follow along and practice on their own computers using "dummy"

[1] https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/
[2] https://cyber-women.com/en/digital-security-basics-1/safe-browsing/
[3] https://cyber-women.com/en/digital-security-basics-1/malware-and-viruses/
[4] https://cyber-women.com/en/digital-security-basics-2/storage-and-encryption/

files created for the purposes of the session (not actually important data or files!)

Leading the Session

Part 1 - Introduction

1. Ask participants how much they value their computers - How useful or essential is it to their personal and work lives? How much information they storage in their computers?
2. Now ask them - How much time do they spend on maintenance of their equipment? The difference between the degree with which people tend to value their devices versus the amount of time they spend on maintenance and care is often quite wide. Explain to the group that this session will focus on basic practices for protecting devices.

Part 2 – Physical Environments and Maintenance

3. Mention to the group that many practices related to device safety are in fact more related to physical security than digital security (this is a good way to reinforce the holistic focus of this curriculum). A good example of this is the importance of cleaning devices – to get rid of dirt or residue that might get inside – and to conduct regular physical inspections of equipment to identify any alterations or physical intrusion attempts. In that regard, you can recommend basic digital practices – like using a password to lock a device if they won't be in its immediate vicinity while it is switched on – as well as physical protections, such as using a keyboard protector or an anti-theft cable chain to prevent unwanted access or theft. Make sure to note here how the most critical aspect of their devices' physical safety: awareness. Being aware of where a device is at any given moment – whether on their person, in the other room, or secured in another location – is essential!

4. Ask each participant to recall the details of their workplace - Which physical risks are present? Is their computer exposed to being stolen? Are there any misplaced cables? Is it possible that their computer might be exposed to extreme heat, cold or moisture? These are other important awareness points – physical awareness isn't just about making sure an adversary doesn't get ahold of their device(s), but also about the potential damage that a device's immediate environment might present.

Part 3 – Software Safety

5. Explain to participants the risks of using pirated software (high likelihood of downloading malware, can't regularly update in the same way as with licensed software, etc.); however, licensed software is also frequently quite expensive. Here, you can share a few resources with the group that will be helpful to address this:

   Osalt[5]

   Open a browser and navigate to Osalt – this is a website that presents free and open source alternatives to many major licensed software platforms and suites (for example, using Ubuntu instead of Windows; LibreOffice instead of Microsoft Word; Inkscape instead of Adobe Illustrator).

   TechSoup[6]

   Via TechSoup, human rights activists and their organizations may be eligible to receive free, or heavily discounted, versions of commercial software: users may look for official distributors among local ICT service providers and request for a non-profit or public sector license discount. A large distribution network for donated software is run by TechSoup - the link above contains a list of partners and the countries in which they operate.

6. Explain to participants the importance of keeping all their software updated - first and foremost, it protects against security vulnerabil-

[5] http://www.osalt.com
[6] http://www.techsoupglobal.org/network

ities. All software and updates should only be downloaded from trusted sources; for example, when updating Adobe Acrobat Reader, one should only use updates downloaded directly from Adobe, not third-party websites.

7. Next, explain to participants the importance of having an antivirus program on their computers - provide some background that can help demystify some of the common myths related to antivirus, such as:

    - Using two or more antivirus programs offers more protection.
    - Mac and Linux don't need antivirus software because they can't get viruses.
    - It's perfectly safe to use a pirated version of antivirus software.
    - Free antivirus programs are not as safe or reliable as paid programs.

8. Share these, along with any others that participants share with you – then, discuss some basic safe practices for using antivirus software and protecting against malware (see Malware & Viruses session in this module). Some useful ones to highlight here, in case you haven't already covered them in the Malware & Viruses session in this module, are:

    - Using the uBlock browser plug-in to avoid clicking on ads that might download malicious malware files onto their computer.
    - Being aware of phishing attempts, suspicious links or attachments found within emails in particular, that appear to be sent from unknown accounts or from accounts that appear similar to those of trusted contacts.
    - This is a good opportunity to mention firewalls – these offer an automated layer of protection in their computers. Share tools like Comodo Firewall, ZoneAlarm and Glasswire. Newer (licensed) versions of Windows and Mac OS also have robust firewalls already installed.

Part 4 – Data Protection and Backups

9. Ask participants - How often do they backup their files? Share examples of best practices related to data backup, such as keeping the backup in a safe place that is separate from their computer, backing up their information on a frequent, regular basis and - depending on the information that is being backed up - to consider also encrypting the hard drive or storage media where data will be stored.

10. Share with participants the backup format template below, and have them start filling it in individually. Explain to the group that this is a useful way of creating a personal data backup policy – they can refer to this after the training, as a useful resource for keeping track of where their data is stored and how often that data should be backed up.

    Backup Format Template

    Type of information

    Importance/Value

    How often it is produced or changed?

    How often must it be backed up?

    ---

11. Explain next that, although there are backup automation tools available (such as Duplicati.com or Cobian), participants may find it easier to start doing their backups by manually dragging and dropping files to the backup storage media. This ultimately depends on the complexity or amount of data they have to manage – for the average user however, manual backups should be more than sufficient.

12. To follow-up on secure data backups, re-visit briefly the concept of encryption for storage media. Explain to the participants what it means to do, and why encrypting their hard drives or storage media can be useful. **VeraCrypt and MacKeeper**, two relatively popular util-

ities for implementing file or disk encryption, could be mentioned here as options for participants to explore.

Part 5 - Deleting Files and Recovering Them

13. Read aloud the following statement:

    > From a purely technical perspective, there is no such thing as a delete function on your computer.

    Ask the group what they think about this – Does this statement make sense? How can it be that there is no such thing as a 'Delete' function? Remind the participants that they can drag a file to the Recycle Bin on their computer desktop, and then empty the bin, but all this does is clear the icon, remove the file's name from a hidden index of everything on your computer, and then tell their operating system that the space can be used for something else.

14. Ask the group - What do you think happens to the data that is 'deleted'? Until the operating system uses that newly free space, it will remain occupied by the contents of the deleted information, much like a filing cabinet that has had all its labels removed but still contains the original files.

15. Now explain that because of how a computer manages this storage space for data, if they have the right software and act quickly enough, they can restore information deleted by accident; likewise, there are also tools available that can be used to permanently delete files (not just remove them from the file index until the space is occupied). Take this opportunity to present **CCleaner, Eraser, and/or Bleachbit** as tools that can be used to delete files and Recuva as an option to recover deleted files.

References

- https://seguridaddigital.github.io/segdig/
- https://securityinabox.org/en/guide/malware

- https://level-up.cc/curriculum/malware-protection/using-antivirus-tools
- https://securityinabox.org/es/guide/avast/windows
- https://securityinabox.org/en/guide/ccleaner/windows
- https://securityinabox.org/en/guide/backup
- https://securityinabox.org/en/guide/destroy-sensitive-information
- https://chayn.gitbooks.io/Avanzado-diy-Privacidad-for-every-woman/content/Avanzado-pclaptop-security.html

Part V

Privacy

Ask me anything!

- **Objective(s):** Explicar cómo nuestros conceptos de privacidad cambian radicalmente en los espacios online.
- **Length:** 15 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Privacy[1]
  - Apps and online platforms: friend or foe?[2]
- **Needed materials:**
  - Slides or cards with questions (see below)
- **Recommendations:** It is important that you share the instructions progressively with participants as you move through the exercise, in the order they are included below – if you provide the instructions all at once before actually conducting the exercise, it will give away the twist!

This session is based on a module developed by Elis Monroy from Subversiones collective for the Voces de Mujeres project.

[1] https://cyber-women.com/en/privacy/privacy/

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

Leading the Exercise

1. Ask participants to choose a partner from the group, and to then find a quiet space for them to talk.
2. Once participants are situated with their partners, ask them to share with each other their answers to the following questions:

- What is the most funny or embarrassing thing that has ever happened to you?
- Mention one thing you hate doing the most.
- Do you have any guilty pleasures with the music you listen to?
- Did you have a nickname when you were a kid?

As the trainer, you can add or change the questions as see fit – the goal is to ask questions that are likely to bring up information or anecdotes that could be a bit embarrassing or funny, and to talk about privacy with participants. There are more personal questions you can use, but be careful which ones you choose depending on your context – you don't want to make participants feel uncomfortable.

3. Once participants are done sharing their answers with one another, have them choose another pair to combine with (there should now be four participants in each group)
4. In the new groups they have formed, ask participants to introduce the partner they worked with during the first round, sharing with the new team members their answers to all the questions.
5. Once the groups of four have all introduced one another's stories, you can now ask participants to join with another group (there should now be eight participants in each group) – they should now repeat over again the process from Step 4.
6. Ask participants how they felt during the exercise. Some examples of issues which participants might raise could include:

- A participant might have shared something because they knew the person they started the activity with at the beginning, or because they felt comfortable in that moment - but they didn't anticipate how the rules of the activity would evolve.

- A participant might have noticed that her partner told one of her stories incorrectly.

7. Close the activity by talking about **privacy**, and how sometimes people agree to the Terms of Service of an online platform without it being clear what the "rules of the game" are, and how they might change over time. Talk also about **consent**, and how a person may sometimes (for instance) agree to have their picture taken, but that doesn't imply that they also agreed (or gave consent) for that picture to be shared online or with other people.

Privacy

- **Objective(s):** Introducing participants to the concept of privacy and identifying information about ourselves that is available online.
- **Length:** 50 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Your rights, your technology[1]
  - Ask me anything![2]
  - Apps and online platforms: friend or foe?[3]
  - Networked publics[4]
  - Doxxing the troll[5]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
- **Recommendations:** Some participants may become unsettled or up-

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

[2] https://cyber-women.com/en/privacy/ask-me-anything/

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

[4] https://cyber-women.com/en/privacy/networked-publics/

[5] https://cyber-women.com/en/online-violence-against-women/doxxing-the-troll/

set by some of the information available about themselves online during the "self-doxxing" part of this session. if this happens, be sure to make plenty of time for the final part of the session where participants will focus on strategizing next steps in response to the information they find. participants should each have access to a device with an internet connection for the practical part of the session.

This session includes information from the "Self-Doxxing and Regaining Control" section of Tactical Technology Collective's manual "Zen and the Art of Making Tech Work for You".

Leading the Session

Part 1 – Do We Truly Have Privacy?

1. Start the conversation by asking participants whether they think privacy truly exists or not. Then, ask them about their own concept of privacy - share your own concept of privacy to provide an example. Transition into the next steps by telling the group that, in this session and during this training, you will all be reclaiming **your right to privacy!**
2. Ask participants to share some examples of factors that could be interfering with the control they have over their data, personal information, and other elements. These could be personal practices, the platforms they trust with their information, the knowledge they have about the tools and devices they use, or the actions of others in their networks.

Part 2 – "Self-Doxxing"

3. Explain to participants what **Doxxing means** – essentially, it's the practice of gathering a substantial amount of personal information about someone and then making it public (usually online). You

should also explain how doxxing is sometimes used against people as a revenge tactic, and is often used to endanger, harass, or threaten activists and human rights defenders.

4. Tell the group that, in this part of the session, they will practice "self-doxxing" as a way to find out how much (and what kind) of information can be found about themselves online. Explain that this is useful preventative measure for taking steps to reduce the available amount of this information (when this is possible).

5. Ask participants to open a blank document on their computers, or to have a piece of paper ready to take notes of what information they discover. Then, have participants launch a browser window on their computers with a browser that is not the one they typically use – this is so they are not automatically logged-in to their various online accounts.

6. Ask participants, before they begin, to make a list of all the public accounts or social media profiles they have; then, ask them to make a list of keywords or phrases that could be linked to them, which could include information such as:

- The city where they were born
- The city where they currently live
- Their home address
- The organization they work for (or organizations they work with regularly)
- Their activism cause
- Major projects or campaigns they work on

7. To begin their self-doxxing, participants should first search for their various online accounts and profiles (these should appear as they would to the general public, since they won't be logged-in), taking note of what information about themselves they are able to find.

8. Next, participants should search for their names and other keywords from the lists they made, using Google and DuckDuckGo as well as Facebook, Twitter, and any other platforms – here are a few additional suggestions for this step:

- For Google and DuckDuckGo, they should do image and video

searches as well as normal searches.

- If they know of any specific online databases - for cities, governments, or otherwise – where their information could potentially appear, they should search those as well.
- If they have their own website, they could search for the domain address at https://whois-search.com to see what information about them is available via the public domain registry.

Part 3 – What Do We Do Now?

9. Explain to the group now that, through their self-doxxing, some may have found information about themselves that they didn't know was publicly available, as well as online accounts they don't use anymore which they may have even forgotten that they had.
10. Ask everyone to look back through the notes they took, and then to think about which next steps they could take to assert more control over what others can find out about them online. Have them each make a "to-do" list of these steps, which could include actions such as closing certain accounts, editing their information and/or privacy setting configurations on social media profiles, enabling private domain registration on their website domain hosting, etc.
11. As participants make their to-do lists, share with them some resources that could be helpful for them as they implement some of these next steps – they may also get inspiration for other steps they hadn't yet thought of:

Temporary URL Blocking Tool Can be used to block search results for websites - does not actually remove content, but blocks older (and potentially more sensitive) content from search results until website(s) can be updated: https://support.google.com/webmasters/answer/1663419?hl=en&lr=all&rd=2

Deleting Facebook Accounts Contains instructions for deleting or disabling Facebook profiles: https://www.facebook.com/help/224562897555674

AccountKiller Has instructions on how to remove accounts or public profiles for most popular websites and social networking services: https://www.accountkiller.com

JustDelete Me A directory of direct links to delete accounts from web services and social networking services: http://justdelete.me

12. To close the session, remind participants that doxxing reveals only the information that is publicly available about them; however, the actual social media platforms and online services themselves can see much more. Emphasize to the group that better privacy is also supported by using stronger passwords, practicing safer browsing habits, and taking advantage of encryption to secure information from others.

References

- https://gendersec.tacticaltech.org/wiki/index.php/Self-dox

Networked publics

- **Objective(s):** Introduce participants to the concept of 'networked publics' to better understand the key issues and implications of technology's expanded role in society.
- **Length:** 20 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Ask me anything![1]
  - Privacy[2]
  - Doxxing the troll[3]
  - What does your metadata say about you?[4]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup

This session is based on Danah Boyd's research.

[1] https://cyber-women.com/en/privacy/ask-me-anything/

[2] https://cyber-women.com/en/privacy/privacy/

[3] https://cyber-women.com/en/online-violence-against-women/doxxing-the-troll/

[4] https://cyber-women.com/en/safe-online-advocacy/what-does-your-metadata-say-about-you/

Leading the session

1. Begin the session by explaining that it is focused on better understanding what happens when technology becomes an increasingly central and essential component of society, and the impact that this has on identity and privacy.
2. Explain that, to illustrate this, you will be featuring some of the key concepts found in Danah Boyd's research, called Taken Out of Context American Teen Sociality in Networked Publics:

    > Networked Publics: Networked publics are simultaneously the space constructed through networked technologies and the imagined community that emerges as a > > result of the intersection of people, technology, and practice.
    >
    > Content of Networked Publics: The content of networked publics is inherently made out of bits. Both self-expressions and interactions between people produce bit-based content in networked publics.
    >
    > Four Properties of Networked Publics: The features of bits configure the four properties that are key to networked publics:
    >
    > Persistence: online expressions are automatically recorded and archived; Replicability: content made out of bits can be duplicated; Scalability: the potential visibility of content in networked publics is great; Searchability: content in networked publics can be accessed through search.
    >
    > These four properties structure network publics and the interactions that take place in them.
    >
    > Dynamics of Networked Publics: Invisible audiences: not all audiences are visible when a person is contributing online, nor are they necessarily co-present.
    >
    > Collapsed contexts: the lack of spatial, social, and tem-

poral boundaries makes it difficult to maintain distinct social contexts.

The blurring of public and private: without control over context, public and private become meaningless binaries, are scaled in new ways, and are difficult to maintain as distinct.

3. Explain and provide examples of each of the four properties, as well as the dynamic. It will help if you can accompany this with images related to each, to make it easier for participants.

References

- http://www.danah.org/papers/TakenOutOfContext.pdf

Apps and online platforms

- **Objective(s):** To focus on the apps and online platforms they use most – you will help them to identify the kinds of information shared with these platforms, and to strategize tactics for using them safely in their personal activities and online activism.
- **Length:** 120 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
  - Personal perceptions of security[1]
  - How does the internet work?[2]
- **Related sessions/exercises:**
  - Ask me anything![3]
  - Privacy[4]
  - Networked publics[5]
  - Safe online campaigning[6]
- **Needed materials:**

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

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

[3] https://cyber-women.com/en/privacy/ask-me-anything/

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

[5] https://cyber-women.com/en/privacy/networked-publics/

[6] https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/

  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
  - Paper (a few sheets for each participant)
  - Post-it Notes (in multiple colors)
- **Recommendations:** Participants should have their mobiles or one device with internet for the practical part of the session. provide participants with further recommended resources where they can learn more about privacy, and steps they can take to better protect theirs (see references section for links).

Leading the session

Part 1 – Our Devices, Our Data

1. Ask participants to go through all the apps they have on their devices and check the following:

    - Which device permissions each app has;
    - Their privacy policies, to see what can be done with the data each app has access to.
    - Who the developer of each app is.

2. Give participants approximately 15 minutes to do the above. Once time is up, ask participants to share what they found in this quick search. Make sure that you cover issues such as:

    - App permissions that have no clear relationship with their actual function;
    - Terms of Service that are unclear or vaguely written;
    - Privacy policies that allow companies to sell user data to third parties.

3. Share examples of “menstruapps” - menstrual cycle tracking apps - and other personal health related apps with the group. Explain how according to research that has been done (via Chupadatos[7]), it’s been

[7] https://chupadados.codingrights.org/es/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros/

shown that menstruapps can gather quite a bit of personal data from users:

- Name, phone number and address
- Bodily details such as menstrual pain, weight, and hours of sleep;
- Emotional states like stress, lack of concentration or anxiety;
- Details about sexual health, including any contraceptive methods;
- Online behaviors like click-throughs and type of devices used;
- Offline behaviors including medicine taken, or habits like drinking or smoking.

That's a lot of information, right?

Part 2 - Who Else is Tracking Us?

4. Split participants into groups of 3-4 participants (maximum) and ask each group to make a list of what they know about Facebook and Google – to provide an example, you can have them start buy answering these questions:

    - Are these entities actually companies?
    - What are these companies' missions or objectives?
    - What are the services they offer?
    - Are those services for free or paid?
    - What are the rules/terms of those services?

    Give participants 15 minutes to finish listing all the information they have.

5. Once time is up, ask each group to then make a list of what these two companies, Facebook and Google, might know about them. If participants have access to internet from their computers or mobile devices, those who have a Gmail account may want to visit the page https://www.google.com/maps/timeline as well to help with this part of the session. Give participants 20-25 minutes to make their lists, which each group should then briefly present to the rest of the participants.

Part 3 – Promoting Women's Rights Using Social Networks

6. For this next part of the session, keep participants in their present groups – you will give each group a question to discuss and work on together (taking from the list below):

    - Which tools or online platforms are we using to organize and exchange information from our social movements, protests and campaigns? What are some of the advantages or disadvantages of using those tools for that purpose?
    - Do we know any examples of censored campaigns, pages taken down from Facebook, videos censored on YouTube or other instances of social media accounts being closed?
    - Companies like Facebook and Google are good friends of our governments, and are known to share users' information with them (https://govtrequests.facebook.com) What are the implications of this?
    - Do we know of any cases of violence against women online? Specifically, any cases involving WHRDs receiving threats online, having their nudes exposed, or social media accounts being created to discredit them or "advertise" their sexual services? On which platforms did these incidents happen, and how did the platform react?
    - Have each group take about 10-15 minutes to answer their question; once time is up, ask each group to share their conclusions with the rest of the participants.

7. Together as a group, take 5-10 minutes to reflect on how these same social networking platforms also serve as gathering places for many online users – as such, they seem to be ideal places to implement campaigning efforts. Ultimately, Facebook and the various services offered by Google provide different useful ways to interact with followers and community members; therefore, despite some of the concerns or disadvantages of these platforms, it's important to remember that many participants may still want to use them to reach out to their audiences.

Part 4 – Reclaiming Privacy

8. You'll now lead participants through the final closing portion of the session. Explain that you will now look at ways to reclaim privacy online, by learning how to continue using these apps, online platforms and social networking sites for personal use or advocacy efforts, but in a safer way.

9. With participants remaining in the same groups as before, ask them to now focus on collaboratively brainstorming creative ways to reclaim their privacy. Give each group a block of post-it notes along with some markers and pens, and have them generate as many ideas as they can think of in 10-15 minutes. You can provide some example tactics to get them started, such as:

    - Confusing the algorithms that platforms use for advertising or content optimization;
    - Regularly checking platforms' privacy policies and updates to privacy settings;
    - Being aware of app permissions on their devices, specifically things like location settings and geo-tagging of photos and posts;
    - Using alternative platforms that are more committed to privacy and activism (Riseup, Tutanota, Signal, etc.)

    Once they've finished this final part of the exercise, have each group share some of the ideas they came up with – you can post these in a visible place in the training room for participants to refer to as they move through the training process. These ideas will also be useful for you as you adjust the content of your training, especially if participants want to focus more on improving their safe use of social networks for their activism.

References

- https://www.kaspersky.es/blog/digital-detox-advices/6226

- https://rankingdigitalrights.org/2017/08/30/rdr-en-espanol-guest-post
- https://myshadow.org
- https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual
- https://www.digitale-gesellschaft.ch/dr.html
- http://www.europe-v-facebook.org

Part VI

Safe online advocacy

Safer websites

- **Objective(s):** To help whrds to identify safer practices to implement for managing and protecting their websites – these could be personal websites that they use for online activism, or the websites of their organizations/collectives/movements.
- **Length:** 50 minutes
- **Format:** Session
- **Skill level:** Advanced
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
  - Familiarity with how websites are administered
  - Who do you trust?[1]
- **Related sessions/exercises:**
  - Who do you trust?[2]
  - Apps and online platforms: friend or foe?[3]
  - Safe online campaigning[4]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
- **Recommendations:** This session will be more relevant for some

[1] https://cyber-women.com/en/trust-building-exercises/who-do-you-trust/
[2] https://cyber-women.com/en/trust-building-exercises/who-do-you-trust/
[3] https://cyber-women.com/en/privacy/apps-and-online-platforms-friend-or-foe/
[4] https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/

groups than for others - prioritize this session especially for women activists or collectives that have a website. it may be a good idea to prepare ahead of this session a few examples (from news reports, blogposts, social media postings or personal experience) of online attacks against whrds and/or whrd organizations, websites hacks or takedowns in particular. remember that in some cases, organizations may not manage their own websites, or their ability to make changes to their websites might depend on the decisions of larger international ngos who support them. either way, even if participants are not able to directly make changes to the processes for administering their websites, this session still provides a solid foundation for them to begin thinking about changes that they might propose (or taking more control over managing their sites).

Leading the session

Part 1 – What Does an Online Attack Look Like?

1. Begin the session by reviewing some of the responses provided during the session Who Do You Trust? (Trust-Building Exercises) – in particular, mention some of the possible adversaries identified by participants. This will provide a useful backdrop for addressing the issue of website safety, especially for women activists in online spaces.
2. Ask participants - What do they consider as an online attack? What are some of the cases of online attacks they have heard about? If appropriate, you may also ask if anybody in the group has been attacked in the past, either individually or in the context of their organization/collective. You can also offer some of your pre-prepared case studies in case participants don't have any examples of their own to share.
3. Pose follow-up questions to the cases that participants (or yourself) have shared - Did the attack happen in the context of a specific event such as a protest, report presentation or another kind of public gathering? What was the response to the attack by the WHRDs involved?

Was any documentation of the attack created?

Part 2 – Protecting and Securing Websites

3. Based on the examples participants have shared, you can now begin to share in turn some initial practice recommendations for improved protection of their websites. Some examples are included below - based on the different levels of knowledge within the participant group, you may want to offer more in-depth explanations for each of these:

Optional: Even for participant groups equipped with some level of knowledge or information about managing websites, before moving on to the below recommendations it may be a good idea to explain the ways in which a website can be administered. Some example topics to mention might include domains and DNS, site hosting, and content management systems (CMS).

Protecting your website

- Use a strong admin password to avoid a website being hacked – adversaries taking advantage of weak passwords to access a website's backend is the most common way that hacking occurs. If possible, activate two-step verification for a website's account, hosting service, and any other portals of access.
- When a domain name is registered, it often requires that person registering it provide information such as their name, address and email. Check to see which information is available on a given domain registration, and consider changing it to a private domain registration (using whois.net is an easy method for checking this).
- Where geographically is a website's domain hosted? There are several things to take consider in this regard, especially:
  - In which country (or even city) are the host's servers located? Can the government of that country be trusted with your data, and more importantly, can the hosting service be trusted not to

hand your data over to a government's request? Could the government of that country attempt to interfere with or attempt to take down a website?

  - Consider if buying your host with the reseller of a reseller is a good option, in some attacks you will need to have a good support team that can help you, so make sure to choose well. Make sure to check that, as some of the hosts options can be well known for having a bad technical support.

- Check the plug-ins that a website currently uses – these are especially common on websites which use Wordpress as a CMS. Be sure to use only the plug-ins that are necessary, and check that any plug-ins currently in use are from a trustworthy source.
- Consider installing utilities like Jetpack by Automattic on WordPress, especially for services like social media widgets, comments and contact forms. There are also basic site security plug-ins available such as Better WP Security[5], as well as plug-ins for automatic data backup such as VaultPress[6] or Backup Buddy[7].
- Make sure to regularly perform updates to a website's hosting servers (if these are not automatically managed by the hosting service), as well as any updates to the CMS, plug-ins, or any other platforms that are used for administration and management.

Protecting your website's visitors

- It is highly recommended that websites offer HTTPS connections to users by default (not just as an option) – Let's Encrypt by the Electronic Frontier Foundation is a service that acts as a certificate authority and offers HTTPS certificates for no cost.
- There are many collectives in operation around the world that support tech activism efforts, and specialize in working with activist organizations - in Latin America for example, Código Sur and Kefir.red

[5] https://wordpress.org/plugins/better-wp-security/
[6] https://vaultpress.com/
[7] https://ithemes.com/purchase/backupbuddy/

are options. Other similar collectives are Austisticy, No blogs and Blackblogs.org.

- If an organization or website has experienced Distributed Denial of Service (DDoS) attacks in the past, consider using the DDoS protection services offered by initiatives such as Deflect or Project Shield. Deflect, which is run by Montreal-based non-profit Equalit.ie, is a completely free service widely trusted in the digital security community.

Optional: Consider sharing resources about responding to a DDoS attack, such as: https://github.com/OpenInternet/MyWebsiteIsDown/blob/dev/MyWebsiteIsDown.md

References

- https://onlinesafety.feministfrequency.com/en/
- https://www.apc.org/
- https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/en

Safe online campaigning

- **Objective(s):** To share digital security recommendations for women human rights defenders who are involved in online campaigning efforts.
- **Length:** 50 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Who do you trust?[1]
- **Related sessions/exercises:**
  - Who do you trust?[2]
  - Gender-based risk model[3]
  - Apps and online platforms: friend or foe?[4]
  - Safer websites[5]
  - Building stronger passwords[6]
  - Malware and viruses[7]

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

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

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

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

[5] https://cyber-women.com/en/safe-online-advocacy/safer-websites/

[6] https://cyber-women.com/en/digital-security-basics-1/building-stronger-passwords/

[7] https://cyber-women.com/en/digital-security-basics-1/malware-and-viruses/

  - How to secure your computer[8]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
- **Recommendations:** The intention of this session is for participants to identify digital security solutions they can implement for safer online campaigning activities; however, the ultimate goal is not for them to implement these during the session, rather it is for them to begin a process of exploration to identify what will work best for their individual context.

This session is based on a guide developed by Indira Cornelio for SocialTIC.

Leading the session

Part 1 – Introduction and Preventative Planning

1. Explain to participants that the intent of this session is for them to identify digital security solutions they can implement for safer online campaigning activities. They won't need to immediately implement these during the session, however - the goal is for them to begin a process of exploration to identify what will work best for their individual contexts and campaigns.
2. Ask participants to share any examples of online campaigns they are aware of – are there any emerging trends in how these campaigns are implemented that they can identify?
3. Remind participants that, when it comes to mounting their own online campaigning and advocacy efforts, they should keep in mind the information and adversaries they identified during the Who Do You Trust? exercise. As campaigns are, by nature, very public efforts, they should be extra aware of who could potentially be monitoring them, or who might potentially pose a threat to them.

[8] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/

4. In the context of their own work, suggest to participants that when it comes time for them to begin the planning phase an online campaigning effort, they should work with their team(s) to answer the following questions:

    - What is the campaign about?
    - What is the key audience? How do they feel about the topic or issue? Are they for or against it?
    - Who might feel targeted or exposed by this campaign?
    - What are potential arguments that could be made against this campaign?
    - What are the best and worst-case outcomes for this campaign?

5. Answering these can help them plan preventative measures against possible threats more strategically – highlight to the group that they can even prepare messaging in advance for possible scenarios that emerge from the responses to these questions. Also, remind participants that even envisioning the best-case scenario of the campaign is helpful for planning preventative measures – for instance, how would they prepare for the possibility that, if the campaign is successful and becomes quite popular, their website is unable to handle a sudden surge in traffic and goes down?

6. Now, explain to the group that during the next parts of this session, you will be providing guidance and recommendations on digital security practices useful for online campaigning efforts (if possible, depending on how much time you have to work with, allow participants to visit recommended tools' websites).

Part 2 – Protecting Devices

7. Ask participants if they use their own personal devices for campaigning (versus a "work" device) - how much campaign related information they store on these devices? Are they connected to email and social media accounts as well?

8. Here are some topline practices to recommend to the group for device protection:

- **Password-protecting** their laptops and mobile phones;
- **Installing antivirus software** on both laptops and mobile phones;
- **Performing regular backups** of important or sensitive data (recorded video or audio, interview notes, reports, etc.) with the backups kept in a safe location separate from their devices;
- **Enabling full-disk encryption** of their devices:
  - For Android and Mac iOS mobile devices, this can be enabled via phone settings;
  - For laptops, Mac OSX FileVault[9] and Windows BitLocker[10] are the most common options for full-disk encryption;
  - Note: Filevault comes for free with Mac OSX; however, BitLocker only comes free with Pro, Enterprise and Education versions of Windows.

Part 3 – Managing Account Access

9. Online campaigns often require multiple users to be able to access the same online accounts (or devices, in some cases). Access to a device or account by multiple users with the same credentials represents a significant increase in risk; however, by taking some preventative measures, participants can substantially reduce the likelihood of these risks becoming direct threats:

    - For all shared online accounts and devices, limiting the list of those with access to as few people as possible is among the most critical first measures to implement; another is to make sure that any protocols or procedures put into place (especially regarding the following recommendations) are followed **regularly and consistently**;

    - For online platforms in particular, all team members with access should make sure to regularly check history and activity on shared accounts – for example, on Gmail/Google

[9] https://en.wikipedia.org/wiki/FileVault
[10] https://en.wikipedia.org/wiki/BitLocker

accounts, they can check the history of recent log-ins (and set alerts for suspicious activity) under "Last Account Activity"; likewise, for Facebook, they can go to the shared account's Activity Log to check on recent activity;

- Apply basic strong password practices for all devices and accounts that will be used for a campaign. Secure password storage managers like KeePass/KeePassX[11] allow individual database files of account passwords to be created, which are in turn protected by a master password; likewise, for accounts like Google, Facebook and Twitter, enabling two-factor authentication provides an additional layer of access control and is highly recommended;
- If a password needs to be shared between team members, but can't be done in person, sending passwords over encrypted email - with GPG or using a service like Tutanota[12] or over encrypted messaging (using Signal on a mobile device) are safer options – if using Signal, make sure to set a protocol with team members about deleting messages with passwords from their devices as soon as they are received.

Part 4 – Choosing Apps for Campaigns

10. When implementing and organizing an online campaign, it is common to use certain apps and tools to keep track of social media/website metrics, or to schedule social media posts. When making decisions about such apps, and which ones to use, there are few questions that participants should keep in mind – these are primarily for them to avoid sharing their information with certain unsafe tools, or tools that are no longer supported by developers:

    - Is the app still active, with developers pushing regular security and feature updates?
    - Does the app have social media accounts that can be followed and interacted with?

[11] http://keepass.info/
[12] https://tutanota.com/

- What are other users saying about the app online and on their social media channels?
- Are there any recent blog posts available about the app?

Part 5 – Community Building through Facebook

11. Facebook is often used in online campaigns to organize communities and to quickly disseminate important messaging and other communications. It is important, however, to highlight some of the potential vulnerabilities are with using these platforms as part of a campaign's core organizing structure:

- Participants should be aware of the implications of using Facebook (or other large social media platforms) could be for their own identities online – to limit their exposure, they should create dedicated profiles specifically for administering pages, rather than using their own personal profiles;
- Note, however, that it is now possible to receive Facebook notifications that are encrypted using a public GPG key to an associated email account – this can be useful for WHRDs who want to take further measures to separate their work and personal identities online while managing campaigns;
- Those who are managing campaigns online should be very deliberate about the kinds of information and communication they share with online platforms like Facebook - there are past examples of campaign Facebook pages and profiles being infiltrated by adversaries, making it necessary for administrators to close them down (or, pages are forcefully shutdown by the platform because of reporting by adversaries)
- This could represent a significant setback to campaign and community building progress, so highlight to participants the importance of having **alternative communication and organizing channels** – these could include:
  - Developing active communities on other platforms simultaneously, so there is always a backup platform to fall back on;

- Users can also download a Facebook page's information to create offline backups, which is a good strategy;
- Using a service like Riseup lists[13] to create email groups for sending out newsletters and other communication;
- Organizing in-person meetups if possible; however, for campaigns addressing certain issues in certain countries, be aware that this may be extremely risky and therefore not advisable;

Part 6 – Informed Consent

12. Discuss the importance of informed consent with the group – this is important generally for awareness raising campaigns on human rights issues, and especially when using images or testimonials of victims, survivors and witnesses of atrocities or other violations in campaign materials:

- Before recording images or video of these individuals, or documenting their stories, they must have explicitly agreed to this beforehand; likewise, they must also explicitly agree to having any of this material **shared publicly** – it should furthermore be made clear to them where and for what purpose these materials will be shared, and what the potential implications could be for them.

References

- http://seguridadigital.org/post/156287966318/consejos-de-seguridad-digital-para-gestionar-redes
- https://archive.informationactivism.org/en/index.html

[13] https://www.lists.riseup.net

What does your metadata say about you?

- **Objective(s):** Introducir el concepto de metadatos y la importancia de tomar conciencia sobre qué metadatos contiene cada tipo de contenidos, especialmente cuando estamos trabajando en situaciones de riesgo en el ámbito de derechos humanos.
- **Length:** 90 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Networked publics[1]
  - Safe online campaigning[2]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
  - Example tools for analyzing and removing metadata
- **Recommendations:** While not required, this session is greatly enhanced for participants if they have already done the networked

[1] https://cyber-women.com/en/privacy/networked-publics/
[2] https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/

publics session. metadata is often one of the more complex topics to introduce in the training process - make sure to budget sufficient time to cover this session in detail, as it is quite critical and relevant to the context of whrds and women activists.

Leading the session

Part 1 - What is Metadata?

1. Begin the session by sharing a few key points with participants – the most important of these are included below:

    - Share a definition of what metadata is, and some common places where participants might encounter it (image files, Word/Excel documents, etc.)
    - Share a few common examples of metadata (date and time of creation, location created, username or author's name, type of device) – you may have participants locate an image or other similar file on their own computers so they can locate its metadata for themselves, or you can share some example screenshots of metadata as it appears in common file formats.
    - Explaining some of the different ways that metadata is created, and how it can be changed or even removed entirely.

    Metadata is often one of the more complex topics to introduce in the training process, so make sure to ask the participants if the concept is clear – if not, take time to answer their questions thoroughly and in detail based on your expertise.

Part 2 - Implications of Metadata in a Human Rights Context

2. When working with WHRDs, it is important to explain what are the pros and cons of metadata – you can succinctly describe this to participants using two key ideas:

Metadata can say a lot about you.

- Ask participants to take a picture with their phones and to check all the metadata that the image file contains - you will need to provide them with a tool such as CameraV to do this, or you may also share a web-based tool like http://metapicz.com if your training is with a very beginner-level group.
- Now, have participants repeat the exercise but with location services disabled on their phones. Split participants up into groups of 3-4 people (maximum) to discuss how they think metadata could be useful, and how they think it could compromise security when performing human rights work.
- In their discussion, keeping the focus on human rights work, it is important that participants also identify under which circumstances metadata found in documents, videos or images help such content be considered as evidence in human rights documentation work. Share with them some practices - such as saving the original files on an encrypted device and creating separate copies for editing or for storing on their computers.

  Metadata is created, but can also be removed.

Share with participants a few options, such as ObscuraCam or Metanull, for erasing metadata from videos and images. If there is enough time left for the session, you might also consider including the option of erasing metadata from documents with LibreOffice.

References

- https://ssd.eff.org/en/module/why-metadata-matters
- https://guardianproject.info/apps/obscuracam/
- https://archiving.witness.org/archive-guide/create/how-capture-metadata/
- https://securityinabox.org/en/lgbti-mena/remove-metadata/

Part VII

Safer mobiles

Marco Polo

- **Objective(s):** Ideal for explaining to participants how a mobile phone works, and how we receive sms messages, phone calls and mobile data on our devices.
- **Length:** 15 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Networked publics[1]
  - Safe online campaigning[2]
- **Needed materials:**
  - Creativity!

This exercise is based on the "Marco Polo" exercise created by Fundación Karisma

[1] https://cyber-women.com/en/privacy/networked-publics/
[2] https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/

Leading the exercise

1. Choose someone from the group to play the role of a “Mobile Phone” – once you have a volunteer, ask her to leave the room.
2. Using the space that you have, divide the rest of the group into “Buildings” and “Antennas” and ask them to distribute themselves throughout the room. Make sure that the antennas are spread evenly, so that each can define their own “quadrant” of the room.
3. Ask the Mobile Phone to come back into the room, and to close her eyes. Explain that she needs to locate all of the Antennas in the room by calling out “Marco” - the Antennas will respond with “Polo” but only if the Mobile Phone passes through their quadrant (the Buildings will remain silent).
4. Have the Mobile Phone attempt to locate all the Antennas by calling out “Marco” – once she has located all of them, you can now explain the basic functions of a mobile phone network:

- Cell carriers operate antennas in different areas, each of which provides coverage for a specific zone (or quadrant);
- Mobile phones receive coverage by sending out a request to new antennas they encounter (“Marco”) as they move from place to place, which antennas then reply to (“Polo”) by providing cell coverage.

Mobile phones 1

- **Objective(s):** To provide participants with an introductory-level overview of how mobile devices function using mobile telephony networks.
- **Length:** 60 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Marco Polo[1]
  - Apps and online platforms: friend or foe?[2]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
  - Paper
- **Recommendations:** This session works best if it is done immediately following the marco polo exercise from this module; however, it can be done by itself as well.

This session is adapted from the activity "How Do Mobile Devices Work?" developed by Alix Dunn (The Engine Room) for LevelUp

[1] https://cyber-women.com/en/safer-mobiles/marco-polo/
[2] https://cyber-women.com/en/privacy/apps-and-online-platforms-friend-or-foe/

Leading the session

Begin by explaining participants the key parts of mobile phones. You can show pictures of each part while explaining them.

Part 1 - What's a Phone Made Of?

1. Although some phones, particularly smartphones, have much more advanced capabilities, all phones share several core components:

Antenna

Antennas, which permit communication between a mobile device and external networks, may be visible on older devices - some significantly older models requiring them to be pulled out manually for use. Most newer phones have the antennas built directly into its body, so they are no longer "visible." Aside from the antenna responsible for communicating with the mobile network, there may also be antennas for WiFi; some manufacturers combine these functions into one antenna for the entire device.

Battery

A battery is what stores energy in order to power a mobile device; in most phones, batteries are easy to remove. In some newer smartphones (notably iPhones and later Samsung Galaxy S models), batteries are not designed for removal and can be hard to access. Removable batteries are preferable for users who use tactics to increase their security.

Baseband Microprocessor

This component manages the communications of the phone, including the communications and commands from the user to the phone, and from the phone to and from the mobile network. The baseband of a phone is usually considered highly "proprietary" by manufacturers and can be considered a

"black box" (inaccessible and not easily tampered with) in terms of its communication protocols, how they are controlled, and other network/device-specific functions. The capability of mobile networks to be able to turn on a phone, identify its location, listen via its microphone, and download data from the device is tied to the baseband on a device.

SIM and SIM Slot

This is where the SIM card is stored in a mobile device. There is a limited capacity for data storage on your SIM card, and some users can decide whether or not they want to save certain data to their SIM, internal phone memory, or to removable media. Mention that some phones are designed to manage multiple SIM cards; other phones operating on non-GSM networks (usually CDMA) do not have any SIM cards.

Removable Media

Removable media are any kind of external memory storage that can be inserted into and removed from a mobile device; these are usually SD-cards and micro-SD cards. Some phones also have Infrared (IR) ports for "beaming" data from one phone to another, as well as Bluetooth functionality.

Cameras

Most phones now have cameras that can take pictures and/or video, in particular smartphones. Many also feature cameras mounted to both the back and front of the device, frequently for use in tandem with video chat applications such as Facebook Messenger or Skype.

Part 2 – Hands-On Practice

2. Ask participants to work in pairs and make a list of risks or threats that involve mobile devices; then, ask them to list some recommended practices they can think of to keep their mobile devices

secure with respect to each of the components mentioned in Part 1 above.

3. Once each pair has finished working, ask them to present their solutions to the rest of the group. Listen for mentions of the following practices and tools in their presentations – if any of these aren't mentioned, make sure to include a brief explanation once everybody is done presenting:

    - Mobile Antivirus
    - VPNs
    - Checking apps configuration
    - Strong Passwords
    - Data Backups
    - Don't charge your phone via USB on public computers

References

- https://securityinabox.org/en/guide/mobile-phones
- https://level-up.cc/curriculum/mobile-safety/how-mobile-networks-work/input/how-do-mobile-devices-work/

Mobile phones 2

- **Objective(s):** Introducir herramientas y recomendaciones para mejorar la seguridad que tienen las participantes, ya familiarizadas con conceptos básicos de seguridad digital, con sus celulares.
- **Length:** 50 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Marco Polo[1]
  - Mobile phones 1[2]
  - Introduction to encryption[3]
  - How to secure your computer[4]
- **Related sessions/exercises:**
  - Marco Polo[5]
  - Mobile phones 1[6]
  - Apps and online platforms: friend or foe?[7]
  - How to secure your computer[8]

[1] https://cyber-women.com/en/safer-mobiles/marco-polo/
[2] https://cyber-women.com/en/safer-mobiles/mobile-phones-1/
[3] https://cyber-women.com/en/encryption/introduction-to-encryption/
[4] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/
[5] https://cyber-women.com/en/safer-mobiles/marco-polo/
[6] https://cyber-women.com/en/safer-mobiles/mobile-phones-1/
[7] https://cyber-women.com/en/privacy/apps-and-online-platforms-friend-or-foe/
[8] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/

- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
- **Recommendations:** If possible, try to know before the training begins what kinds of phones participants use – for instance, this could be a question on a pre-training assessment survey. this will help you tailor your session content to the specifics of the devices/operating systems participants already use. before you start the session, remind participants of some basic digital security practices that can be implemented for mobile phones such as: mobile antivirus software, mobile vpns, checking app settings and permissions. **have participants perform a backup of the files they have on their devices before starting this session!** since they will be using their own devices for this session, it is important that they back their data up just in case.

Leading the session

Part 1 – Encryption for Mobile Devices

1. Remind participants of previous sessions that have touched upon the concept of encryption, especially the Introduction to Encryption session – you may have also discussed encryption previously in the context of full disk encryption during the How to Secure Your Computer session. Note to participants that the latest versions of iOS and Android (May 2017) now have encryption turned-on by default.

Part 2 – Using GPG on a Mobile Device

2. If participants are already familiar with GPG encryption, introduce them to the K-9 email client and to APG. Discuss the pros and cons of using GPG on a mobile device (especially the risk of keeping a private GPG key stored on a smartphone versus the unique vulnerabilities of mobile devices) – the idea here is to reinforce that these decisions can vary from one context to another; participants will need

to decide on their own whether the pros of using GPG on a mobile device outweigh the cons.

Optional: Give participants time to install and practice using K9 and APG during this session - they may want to try using the new key-pairs that they create as they get familiar with the tool.

Part 3 - Is Your Phone Tracking You?

3. Ask participants - How much information do our phones know about us? Phones are a medium for many of our conversations, and thus have access to most if not all their contents; likewise, phones also keep track of not just content but also contacts – every conversation can be connected to specific individuals.
4. You may also want to discuss with participants how the kind of tracking a phone performs could be considered a form of surveillance, and how surveillance can take place through more than just the usual, anticipated methods. Ask the group about what kinds of threats or risks they feel might be posed by their mobile devices, specifically in the context of their work as WHRDs.

References

- https://securityinabox.org/en/guide/mobile-phones
- http://www.zeit.de/datenschutz/malte-spitz-data-retention

Part VIII

Anonymity

Secret friend

- **Objective(s):** Explicar el concepto de anonimato y dirigir una sesión práctica que genere mayor conciencia sobre su relevancia.
- **Length:** 30 minutes
- **Format:** Ejercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Anonymity[1]
  - More online identities![2]
- **Needed materials:**
  - Pens, letter stationary and envelopes
  - Chairs
  - A bowl (or jar)
  - Small slips of plain paper
  - A blindfold or other object to cover the eyes
- **Recommendations:** It is strongly encouraged to give participants notice of this exercise ahead of time and what it entails. because time during the training is limited, the exercise is best delivered if participant have already had some time to think about the identities they

[1] https://cyber-women.com/en/anonymity/anonymity/
[2] https://cyber-women.com/en/anonymity/more-online-identities/

will create and can thus come prepared with those details already in mind.

Leading the exercise

Part 1 - Introduction

1. In this exercise, each participant will share an entirely new identity for herself, which they will have prepared ahead of time – it must be completely made up and not based on a real person.
2. Explain that in building this new identity, participants can exercise complete freedom: they can be women, or men, or even a place - whatever they come up with. The key here is to develop their new identity to the full extent possible – this means developing everything from their name and where they come from, to their work, family and even hobbies.

Part 2 - Time to Play!

3. Once you've introduced the exercise, begin the next step by introducing briefly the concept of anonymity. Ask participants why they think anonymity could be important to the work that they do, as well as to their personal lives or relationships.

Once you've completed the introduction and overview of anonymity, the exercise itself should be facilitated using the following steps:

4. Each woman must arrive to the exercise with an already well-defined concept of their new identity - everything from their name and where they come from, to their work, family and even hobbies, etc. Before the exercise begins, have each participant share with you the name of their new identity so you can keep track (this will be important for the exercise).

5. Everyone must write on a slip of paper the name they have chosen for their new identity. Collect each of the slips and place them in a bowl.

6. Walk around the room and allow each participant to draw one name from the bowl - if they take their own identity, they should put it back and draw another slip of paper. The name that each participant draws will be their secret friend.

7. Everybody should now take a few minutes to write their secret friend a letter describing (from the perspective of their own created identity) who they are, where they are from, what their hobbies or work are, etc.

8. Once they have finished writing their letters, they will place them inside an envelope. The name of their secret friend should be written on the outside of the envelope. Make sure that participants aren't able to see each other as they write, to avoid giving away any details.

9. Go around the room and collect each envelope – referring to your list of which identity corresponds to which participant, pass each letter back out to their intended recipients (again, making sure that participants can't see the names written on any of the envelopes other than the one that is intended for them).

10. One by one, invite each participant to the front of the room, where they will sit on a chair and put on a blindfold. They will then share the details of the letter they received, including the name of their secret friend.

11. As each participant describes their letter, their secret friend should get up and sit in another chair that has been placed next to the volunteer.

12. When each participant finishes describing their letter, ask her to guess who from among the other participants they think their secret friend is. Once they guess a name, remove the blindfold and tell them to look at who is sitting next to them to see if they guessed correctly.

13. Continue the exercise, repeating the process above until all identities are discovered.

Part 3 – Closing Circle

13. Once the exercise has completed, ask the group – did they guess correctly who their secret friend was? How were they able to guess, or what was their thought process for attempting to guess? How difficult was it for them?
14. Close the exercise with a reflection on the importance of anonymity and being able to fully protect one's identity, but also how easy it can sometimes be for others to hide their true identities (as well as their intentions).

Anonymity

- **Objective(s):** To introduce participants to the concept of online anonymity, along with relevant tools and practices that can help preserve this anonymity.
- **Length:** 40 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
- **Related sessions/exercises:**
  - Secret friend[1]
  - What does your metadata say about you?[2]
  - Safe browsing[3]
  - More online identities![4]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup

[1] https://cyber-women.com/en/anonymity/secret-friend/

[2] https://cyber-women.com/en/safe-online-advocacy/what-does-your-metadata-say-about-you/

[3] https://cyber-women.com/en/digital-security-basics-1/safe-browsing/

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

Leading the session

Part 1 – Introduction to Online Anonymity

1. Start the session by asking participants – What does anonymity mean to them? After you've heard a few answers from the group, present the concept of anonymity in more detail to the group, explaining the following:
    - Explain what the benefits of learning more about anonymity are, and why it can be relevant to human rights work;
    - Provide examples to participants of online data traces that could potentially identify somebody – these could include data such as a username, social media posts, devices used, locations, and other kinds of metadata;
    - Talk about how anonymity can be applied in levels or layers, explaining to participants that they can anonymize either a single activity or connection, or an entire profile or user session.

Part 2 – Identifying Data and Preserving Anonymity

2. In the previous part of the session, you discussed the different kinds of online data traces that could potentially identify somebody. Now, you will highlight one that is especially relevant to an online context – the IP address:
    - What is an IP address? Explain to participants what it is, its purpose, and how in an online context it can be an especially crucial piece of information (especially when attempting to navigate anonymously in online spaces);
    - To demonstrate some of the anonymity implications of IP addresses to the group, have them use a website like What's My IP Address[5] to find out their individual IP addresses, and how

[5] https://whatismyipaddress.com/

they reveal other kinds of potentially sensitive or identifying information.

3. Now, you will present the following tools to participants and explain how each is important to preserving anonymity online – note that each one provides anonymity in a different way or to a different level:

    - Tor Browser
    - Virtual Private Network (VPN)
    - Tails (The Amnesiac Incognito Live System)
    - HTTPS Everywhere

    It is important to explain some of the key practices to consider to use each of the above tools safely, and to allow enough time for participants to install and practice using them.

Part 3 – Some Hands-On Practice

4. Ask participants to check again their IP on What's My IP Address[6] - they should do this once while using a VPN, and a second time while using Tor Browser. Do they notice a difference in the IP address, or with anything else?

5. This is a good opportunity to address another point of frequent confusion for users: Incognito Mode. Many times, users think they are browsing anonymously while using Incognito Mode on their browsers – here, you should ask participants to check their IP address while using only Incognito Mode (or its equivalent, depending on which browser they are using). What do they notice about their IP address now?

[6] https://whatismyipaddress.com/

More online identities!

- **Objective(s):** Sharing examples of cases, tools and good practices for creating online identities.
- **Length:** 120 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
  - Anonymity[1]
  - What does your metadata say about you?[2]
  - Safe browsing[3]
- **Related sessions/exercises:**
  - Anonymity[4]
  - Secret friend[5]
  - What does your metadata say about you?[6]
  - Safe browsing[7]

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

[2] https://cyber-women.com/en/safe-online-advocacy/what-does-your-metadata-say-about-you/

[3] https://cyber-women.com/en/digital-security-basics-1/safe-browsing/

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

[5] https://cyber-women.com/en/anonymity/secret-friend/

[6] https://cyber-women.com/en/safe-online-advocacy/what-does-your-metadata-say-about-you/

[7] https://cyber-women.com/en/digital-security-basics-1/safe-browsing/

- **Needed materials:**
  - Laptop/Computer and Projector setup
  - Flipchart paper (1-2 sheets per participant)
  - Markers or pens

This session is based on the guide "Creating and Managing identities Online" from Tactical Technology Collective's manual "Zen and the Art of Making Tech Work for You".

Leading the exercise

Part 1 – Connected Online Identities

1. Begin the exercise by having participants make a list of any online identities they have; you may also simply ask the group if anyone among them currently uses more than one online identity. For any participants who indicate that they manage multiple online identities, ask them if they would be comfortable sharing their reasons for doing so with the rest of group and what they use them for.
2. Building off any examples shared by the group, explain that using multiple online identities is not an uncommon practice among WHRDs – offer some example scenarios:
   - WHRDs who use Facebook to manage online campaigns, but don't want to use their personal profile or identity to administer the campaign's page;
   - WHRDs who conduct sensitive research online, and want as few of the digital traces they leave behind to be traceable back to them;
   - WHRDs who have been documenting cases of government human rights abuses, and are planning to expose this information by publishing a major report or public statement.
3. Now ask participants to gather in pairs and identify other circumstances under which it might be useful for them to create a new identity that is not linked to their personal one. Have them reflect

on how much they combine their personal identities with their activism work:

- Do they mix their accounts? Do they mix their identities?
- How linked is their personal digital life with their activist life?
- What are some online activities that could put them at risk of exposing themselves if done using their real identities? Examples of this might include:
- Requesting information from government agencies;
- Visiting government websites to gather information to share online;
- Managing the social media account(s) of their organization or collective);

Part 2 – Separating and Managing Online Identities

4. Again building off the group reflections from the previous step, illustrate to the group three options for managing their online identities:

    - Creating an entirely new, fake online identity;
    - Creating separate personal and professional profile identities;
    - Leaving their identity as it is now (not changing anything);

5. Provide for each of the above options at least one real-life, relevant example and explain to participants what each of these options implies, for example:

    - Creating an entirely new, fake online identity will most likely require it to be completely disconnected from anything that could be related back to your real identity to be effective. This means creating new email addresses and social media handles, needing to consistently log in and out of these accounts to ensure there is no identity crossover, and (with social media handles) very likely starting from scratch with zero followers;

    - Separating professional from personal identities may only require users to change privacy configurations on their accounts, either to limit the amount of information that is available publicly, or to specifically manage what level of information is vis-

ible to specific friends, followers or contacts; in other cases though, separating these identities could imply the need to maintain entirely separated set of profiles and accounts for each (meaning that a new set would need to be created for either the personal or professional identity).

- Leaving an identity as it is would likely only require users to change privacy configurations on their accounts, either to limit the amount of information that is available publicly, or to specifically manage what level of information is visible to specific friends, followers or contacts.

6. Now, ask participants to discuss in their same pairs (from Step 3) what some of the pros and cons of each of these options could be, either in a general sense or specifically for themselves and their context. Among the issues that will likely arise during these discussions are those of practicality and credibility – be prepared to speak to those questions specifically when participants share some of their discussion takeaways with the group.

Part 3 – Hands-On Practice and Recommendations

6. Explain to participants that they are welcome to choose any of the three options presented for the next part of the exercise (the steps below though will use the example of creating an entirely new identity).

7. Give each participant 1-2 sheets of flipchart paper and some markers, and ask them to start drafting characteristics of their new identity – some specific considerations for them to think about include:

   What is the name they would use? (Be aware that some social media platforms, notably Facebook and Google, can identify and take down accounts with fake names, so participants should think creatively);

   What would their interests and hobbies be?

   Where are they from and where do they live?

   What avatar or profile photo would they use?

Could any of these details be traced back to their real identities?

8. Once participants have drafted the details of their new profiles and identities, share with them some digital security recommendations that will help them avoid exposing their reali identities. Note that some of these recommendations were largely covered already in the previous required sessions (Anonymity, What does your metadata say about you? and Safe browsing), and will serve more as a review:

   Using a disposable 'burner' phone for new accounts and profiles – Google requires a phone number to send verification codes during the account setup process, and a phone number is also required to setup two-factor authentication for many platforms (two-factor authentication is highly recommended for securing these accounts) – allows users to provide a number that is not their primary one in these cases.

   Using different machines or devices for each identity – similar to the above, this further compartmentalizes their different identities and separating activities, helping users avoid mistakes that could compromise a new identity. Participants could do this by using separate physical computers or phones, setting up a separate virtual machine on their laptops, or by using an alternative operating system like Tails (see the session Let's Reset! for more information);

   When setting up a new profile, and ideally when logging into the associated accounts in the future, participants should consider using a separate browser different from the one they primarily use for their current profiles – this will help them to avoid linking the accounts, or accidentally logging into one over the other and sharing information that could compromise the separation of their identities;

   Review general safe browsing habits with participants – you could build on this by talking about the concept of browser 'fingerprints', and the impact that could have on the separation of their identities https://panopticlick.eff.org/static/browser-uniqueness.pdf; furthermore, you could also review how to obscure IP addresses that could potentially reveal location details;

   Participants should not follow anybody friends, family or their organization using their new identities – this could very quickly allow

anyone looking closely enough to draw a connection between that identity and its real counterpart;

Remind participants to be aware of metadata and how it could potentially reveal information about themselves. Review how metadata is created, and how they can erase it from their files before posting images or videos, or before sending files from their new identity accounts.

9. Now participants can begin creating the profiles and accounts for their new online identities!

References

- https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual#Creating_and_managing_identities_online

Part IX

Encryption

Introduction to encryption

- **Objective(s):** To explain to participants the concept of encryption, as well as a brief overview of the different types of encryption available to users.
- **Length:** 50 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
- **Related sessions/exercises:**
  - Privacy[1]
  - Safe online campaigning[2]
  - Encrypted communication[3]
  - Storage and encryption[4]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
  - Examples of encryption techniques (printed)

[1] https://cyber-women.com/en/privacy/privacy/
[2] https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/
[3] https://cyber-women.com/en/encryption/encrypted-communication/
[4] https://cyber-women.com/en/digital-security-basics-2/storage-and-encryption/

Leading the session

Part 1 - Have You Used Encryption Before?

1. Explain that this is an introductory session for encryption as a concept, so you will not yet be going into great depth on any of the encryption tools that participants have likely heard about before (GPG/PGP in particular).
2. Split participants up into pairs, and then start the session by demonstrating a few examples of encryption techniques. Here are a few examples that you can prepare ahead of time to share with the group:

The BLUEPRINTS Code

Each of the letters in the word Blueprints is assigned a number.

```
B  L  U  E  P  R  I  N  T  S
0  1  2  3  4  5  6  7  8  9
```

This is a specific example using a specific word, but can be broadly applied to any number and letter sequence - for instance, if you use the same system as above, the sequence of numbers 8 2 5 7 9 would spell T U R N S when “decrypted”.

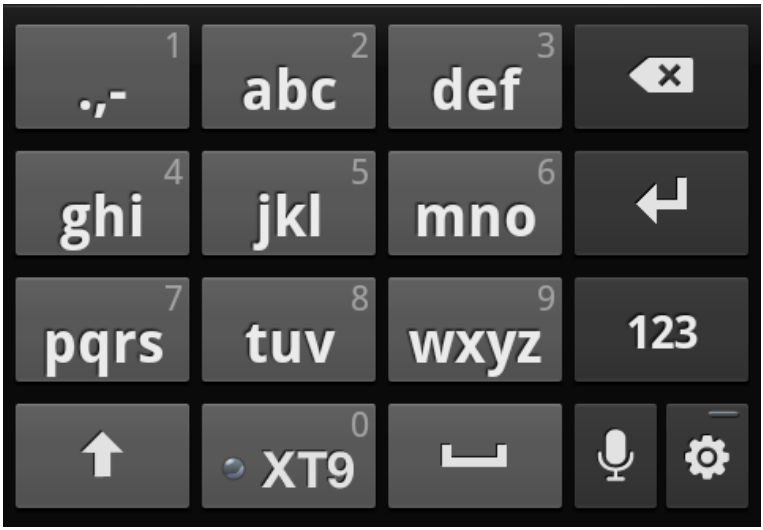
You could also switch the order of the numbers, so that instead of the above sequence, it now goes:

```
B  L  U  E  P  R  I  N  T  S
9  8  7  6  5  4  3  2  1  0
```

In this instance, the sequence of numbers 8 2 5 7 9 would now spell L N P U B (which isn’t a word) when “decrypted”; however, you could now “decrypt” the sequence 4 3 2 0 6 as R I N S E.

Old-Fashioned Text Messaging

Use an image of an older-style phone keypad (see below) to demonstrate another kind of "encryption" that participants may be familiar with.



Old-Fashioned Text Messaging

Ask participants how they would use this keypad to spell different words – one example you could use would be to have each participant explain how they would use the keypad to spell their name. For instance, a participant named Luisa would spell her named by typing the sequence 5 5 5 8 8 4 4 4 7 7 7 7 2.

3. Once you've completed the above examples, ask participants if they have ever used other kinds of encryption – either like the above, or any other examples they can think of (e.g. a common instance of encryption used by many people every day is HTTPS).

4. Close this part of the session by following-up with another question: What are the common elements they can identify from these different examples of encryption?

Part 2 - Explaining Encryption

5. Building on the common elements of encryption identified by participants in Part 1, you should now expand on some further basics and practices for the group:

   Encryption Methods: Take time to explain how encryption works, referring back to the examples from Part 1 as well as by showing a few example screenshots of what a GPG-encrypted email looks like. Highlight common implementations of encryption – in particular, spend time reviewing HTTPS, end-to-end encryption and GPG/PGP encryption.

   Keys and Keypairs: Explain how encryption keypairs work, and the algorithmic relationship between public and private keys. Go back through the example implementations previously mentioned (HTTPS, end-to-end and GPG/PGP) and explain for each of these where their respective keys are stored and/or visible to the user.

   Encryption Practices: Highlight some of the critical best practices associated with common implementations of encryption, such as fingerprint verification and key-signing. To demonstrate, ask participants to locate where within Signal one can verify another user's fingerprint; similarly, if participants already have GPG/PGP keys you can discuss the benefits and disadvantages of signing and distributing public keys. This is also a good time to discuss end-to-end encrypted messaging for chat apps such as Signal, Telegram and Whatsapp – remind participants that end-to-end encryption on some of these services is not always enabled by default.

   Encrypted Backups: Building off the GPG/PGP example above, ask participants whether they think it is a good idea to backup their GPG private key, and if so, how might they go about doing so?

References

- https://www.gnupg.org/gph/en/manual/book1.html

Encrypted communication

- **Objective(s):** To convey to participants the importance and utility of encrypting communications and providing relevant tools.
- **Length:** 50 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
  - Introduction to encryption[1]
- **Related sessions/exercises:**
  - Introduction to encryption[2]
  - Privacy[3]
  - Safe online campaigning[4]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup

[1] https://cyber-women.com/en/encryption/introduction-to-encryption/
[2] https://cyber-women.com/en/encryption/introduction-to-encryption/
[3] https://cyber-women.com/en/privacy/privacy/
[4] https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/

Leading the session

1. Start the session by sharing relevant examples of situations where encrypted communications could be useful, taking time to explain how encryption works. Demonstrate some example screenshots a GPG-encrypted email to illustrate roughly what messages and emails look like while encrypted, and highlight common implementations of encryption – in particular, HTTPS, end-to-end encryption and GPG/PGP encryption.
2. Focus the discussion now specifically on tools that permit encrypted communications: Signal for calls and messages, meet.jitsi for video calls and Tutanota or GPG & Thunderbird for emails are good examples to share.
3. Explain the security benefits of these tools to the group, primarily how they enable users to limit others' access to their communications; then discuss situations where the security of a user's data could still be compromised, even while using encrypted communication. Ask participants – How could the contents of a GPG encrypted email be compromised by keylogging or screen-capturing malware? What if a user's private GPG key was accessed by an adversary – how could they use it to gain access to their data?
4. If time allows, participants should have the opportunity for hands-on practice with at least one of the tools mentioned above in Step 2. Although there may not be enough time to set the group up with GPG/PGP for email, you may choose to demonstrate an HTTPS protected video call using meet.jitsi, or have participants install Signal on their phones to practice sending one another encrypted messages, or to exchange encrypted phone calls.

References

- https://ssd.eff.org/en/module/how-use-signal-android
- https://ssd.eff.org/en/module/how-use-signal-ios

Part X

Digital security basics 2

Storage and encryption

- **Objective(s):** To reinforce the importance of regularly backing up data to participants, and discuss how they can prevent unauthorized manipulation or access to their information..
- **Length:** 90 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
  - Introduction to encryption[1]
  - How to secure your computer[2]
- **Related sessions/exercises:**
  - Privacy[3]
  - Safe online campaigning[4]
  - Introduction to encryption[5]
  - How to secure your computer[6]
- **Needed materials:**
  - Slides (with key points included below)

[1] https://cyber-women.com/en/encryption/introduction-to-encryption/
[2] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/
[3] https://cyber-women.com/en/privacy/privacy/
[4] https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/
[5] https://cyber-women.com/en/encryption/introduction-to-encryption/
[6] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/

  - Laptop/Computer and Projector setup
  - Printed copies of the Backup Format Template (see below)
  - USB drives or other type of storage media (for each participant)
- **Recommendations:** This session will have participants using either veracrypt or mackeeper (depending on their operating system) to practice encryption of data backups and storage media – to save time, consider having participants download either of these ahead of time. in general, and especially for beginners, it is not advisable for participants to perform a full-disk encrypt of their computer hard drives just yet – rather, they should test out veracrypt or mackeeper on external storage media (such as a usb drive) using dummy files that they have prepared specifically for this session. you don't want to run the risk of a participant accidentally losing access to any data during the training!

Leading the session

Part 1 – Data Backups and Planning

1. Ask participants - How often do they backup their files? Share examples of best practices related to data backup, such as keeping the backup in a safe place that is separate from their computer, backing up their information on a frequent, regular basis and - depending on the information that is being backed up - to consider also encrypting the hard drive or storage media where data will be stored.

2. Share with participants the backup format template below, and have them start filling it in individually. Explain to the group that this is a useful way of creating a personal data backup policy – they can refer to this after the training, as a useful resource for keeping track of where their data is stored and how often that data should be backed up.

   Backup Format Template

   - Type of information
   - Importance/Value

- How often it is produced or changed?
- How often must it be backed up?

Part 2 – Storage and Backup Encryption

3. Now that participants have filled out the backup format template, ask them to review the types of information (and their respective importance or value) on their lists again – as they do so, have them consider what might happen if that information were to fall into the hands of an adversary, or if they were to lose that information entirely. What kind of impact would this have on them personally or on their organization?

4. Now, introduce the concept of encryption to the group – explain that they likely encounter encryption quite often in their daily routines, as it is used in different ways across different tools and platforms. You can share, for instance, that HTTPS is itself a form of encryption for data "in transit" (data enroute from point A to point

    B) whereas in this session, you will be discussing encryption for data "at rest" (data that is being stored in one location).

5. Remind participants about how they were asked to download either Veracrypt or MacKeeper onto their computers. Give participants time to install and test out these tools, using external storage media (such as USB drives) and dummy files that they have prepared specifically for this session. Especially for beginner level participants, it is not advisable to do a full-disk encrypt of a computer hard drive just yet - you don't want to run the risk of a participant accidentally losing access to any of their data during the training!

References

- https://securityinabox.org/en/guide/veracrypt/windows/
- https://securityinabox.org/en/guide/veracrypt/mac
- https://securityinabox.org/en/guide/veracrypt/linux

Let's reset!

- **Objective(s):** To reinforces the idea that "tools and technology don't have magic superpowers over us!" here, you will lead participants through an empowering process of "starting from scratch" by resetting their devices and getting a fresh start.
- **Length:** 90 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
  - Introduction to encryption[1]
  - Storage and encryption[2]
- **Related sessions/exercises:**
  - Personal perceptions of security[3]
  - Malware and viruses[4]
  - Privacy[5]
  - More online identities![6]

[1] https://cyber-women.com/en/encryption/introduction-to-encryption/

[2] https://cyber-women.com/en/digital-security-basics-2/storage-and-encryption/

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

[4] https://cyber-women.com/en/digital-security-basics-1/malware-and-viruses/

[5] https://cyber-women.com/en/privacy/privacy/

[6] https://cyber-women.com/en/anonymity/more-online-identities/

  - Storage and encryption[7]
- **Needed materials:**
  - Slides (with key points included below)
  - USB drives live-configured with bootable Tails and Ubuntu OS
- **Recommendations:** Consider bringing each participant a live usb for them to keep; otherwise, have a computer prepared for participants to practice on (or two, if demonstrating both tails and ubuntu) - even if the activity is just intended to run tails or ubuntu from a live usb instead of installing it, some participants not feel comfortable using their own computer to test these out. this can also be readily adapted into a session for any fearless activist women in your training who want to try changing operating systems completely, from mac os or windows to a linux distribution such as ubuntu.

Leading the session

Part 1 – Dispelling the Myth

1. Begin by explaining the goal of this session: to re-affirm the power that humans have over technology, dispelling the notion that digital devices have "superpowers" over their users. If you did the session Personal Perceptions of Security with participants, you can remind them of the following from the closing affirmations:

   > 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!

Part 2 – So What Do We Mean by Resetting?

2. Repeat to the group the affirmation from the previous step, highlighting the final phrase "we can always reset them" – what does this mean? Explain by presenting the following scenario:

[7] https://cyber-women.com/en/digital-security-basics-2/storage-and-encryption/

- Perhaps at some point along your digital security journey, you've felt as though you'd been doing everything wrong.
- You look at your computer – it's full of pirated software, torrented movies and TV shows, and cluttered with other files you don't even remember downloading.
- You've used USB sticks indiscriminately - on your laptop, on computers and printers at cybercafes, and maybe you don't even always eject when you're finished using them.
- Perhaps you've just ended a relationship with someone who you know for sure was looking on your computer when you weren't around – they probably guessed your password, or maybe you even told them what it was.
- Now, you feel like you're out of control – who knows what kind of viruses are living inside your hard drive, or who might have access to your information?
- But guess what – it's okay! It's not too late to get a fresh start. Want to start over? This session is for you!

3. Now, having read through the above scenario for context, you can explain what is meant by resetting in this context: it means starting from scratch, by resetting your device or your computer to its default condition and configuration, and thus giving yourself a "blank slate" for your digital security process.
    - Be sure to remind participants that this session will explain how to perform a reset - they will not actually need to perform the reset during the session, or even during the training.
    - Resetting can go seriously wrong if participants are not prepared, or haven't done a backup of their data in recent days – they also likely still need to use their laptops as they currently are to maintain access to their data until they can better prepare.
    - However, during this session participants will have the opportunity to practice using alternative operating systems on their

laptops, which will be an important point of preparation if they do decide that they would like to perform a reset at some point.

Part 3 – Check-In: Do You Need to Backup?

4. Ideally, you will have already covered the session Storage & Encryption with participants as it addresses important points regarding data backup. Either way, before you begin the hands-on practice portion of this session, do a quick check-in with the group about backing up their data.

   Optional: As a quick refresh from Storage & Encryption, ask participants - How often do they backup their files? Share examples of best practices related to data backup, such as keeping the backup in a safe place that is separate from their computer, backing up their information on a frequent, regular basis and - depending on the information that is being backed up - to consider also encrypting the hard drive or storage media where data will be stored.

Part 4 – Resetting & Rebooting

5. Before you begin the hands-on practice portion of this session, another important point to address is the relationship between rebooting and resetting, two terms which may have been used interchangeably during this session:

   - They refer to very similar processes in a general sense, but remind participants that "reset" is being used to illustrate the concept of "starting over" in the context of this session.
   - A reboot is a technical operation that will be performed by their computers during their reset; it is also an important process to understand for the hands-on practice with alternative operating systems that will occur in the next part of the session.

6. To further clarify the above point, while also providing some valuable technical insight to participants which will be helpful for the

next part of the session, introduce Tails and Ubuntu. Explain how Tails and Ubuntu are alternatives to operating systems like Mac OS and Windows – for this session, the hands-on practice portion will focus on running these operating systems from a USB drive.

Part 5 – Live Operating Systems

7. You may get a question now, which sounds like the following: How can we use a new operating system on our laptops without getting rid of the one we already have? What about our data? You should now take this opportunity to explain to participants a few vocabulary terms that will help them understand more clearly how Tails and Ubuntu operate in the context of this session:

Live System

A live system is an operating system which can be run directly from an external media storage device such as a USB stick or SD card. Tails - which stands for The Amnesic Incognito Live System - is one such example; Ubuntu, which is another "flavor" of the Linux-based operating system that Tails uses, can also be configured as a live system.

Linux

Linux is an operating system similar to Windows or Mac, the major difference being that it is distributed as free and open-source software. Because of this, there are many different adapted distributions of Linux available - Debian, one of the more popular distributions, forms the foundation for Tails.

Boot(able) Device

A Boot (or Bootable) Device is a device or drive from which a computer loads files in order to actually start. For example, on many computers the hard drive is the boot device from which an operating system (such as Windows)

is loaded when you turn a computer on. Aside from hard drives, media like CDs, DVDs, SD Cards, and USB flash drives are also boot(able) devices.

BIOS

BIOS (Basic Input/Output System) is the first software many computers run when they are switched on, used to run self-tests on systems and hardware to ensure they are working properly, and to initiate the load sequence for software (like an operating system) located on available bootable devices. BIOS has an interface, but users cannot access it unless they take specific action during startup to access it directly.

Boot Sequence

The boot sequence, which can be accessed through BIOS (or UEFI) during startup on a computer, is a list of the bootable devices on a computer - it is used to determine the order in which a computer attempts to load information from these devices. Normally, a computer's hard drive is the first device in the boot sequence, from which the operating system is loaded. However, the boot sequence can be changed to first load information from external, removeable devices like DVDs or USBs.

Part 6 – Hands-On Practice

8. To begin the hands-on practice component of the session, divide the participants into at least 2 groups. Provide each group with a computer for them to try running Ubuntu or Tails from a pre-configured live USB; alternatively, if you have enough pre-configured USBs for all participants, they can each practice on their own (in this case, you will want to have everyone practice using either Tails or Ubuntu)
9. On your own laptop or computer, using a projector, walk participants through the process of rebooting their computers and launching Tails/Ubuntu during the BIOS boot sequence. As you do this, be sure to explain the differences between Tails and Ubuntu so that the

group more clearly understands how they can be used to do their own “reset”.

10. Close the session by discussing how resetting using Tails or Ubuntu can be an option for starting a “blank slate” on participants’ computers in the event of a malware attack or other loss of control, but also be sure to mention other types of attacks where this solution does not apply as readily, such as online violence.

References

- https://tails.boum.org/
- http://www.ubuntu.com

Part XI

Online violence against women

Spectogram

- **Objective(s):** To provide a useful way for participants to know each other's thoughts on specific issues, by creating a live spectrum of opinion in the training space.
- **Length:** 90 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - A feminist internet[1]
- **Needed materials:**
  - A large room or outdoor space
  - Yourself!

The content for this exercise was developed by Mariel Garcia (SocialTIC) and Spyros Monastiriotis (Tactical Technology Collective)

[1] https://cyber-women.com/en/online-violence-against-women/a-feminist-internet/

Leading the session

1. Begin by indicating for the group where the two ends of the Spectrogram "spectrum" are located – if using an indoor space, these can be opposite ends of a room; for an outdoor space, it could be two trees, walls or other points.
2. Explain that each of the two ends represents a general opinion – indicate that one end will represent "Strongly Agree" and the other will represent "Strongly Disagree".
3. Now, explain how the exercise will work – you will read out a statement (it is important that these be phrased as statements and not questions), and then repeat it; then, participants will arrange themselves along the "Strongly Agree – Strongly Disagree" spectrum in a way that represents how strongly they feel about the statement you've just read.
4. Remind participants that they don't need to choose only one end of the spectrum or the other; they can stand at the exact middle point if they are undecided on their opinion, or they can stand along any other point that indicates the extent to which they Agree or Disagree with the statement.
5. In this Spectrogram, you will be reading aloud several statements related to digital security and women's online experiences – here below are examples of statements you can use:

- There is no good reason for anyone to share their email/social networks password.
- Sometimes it is necessary for us as women to avoid sharing certain opinions online.
- Women and men activists face the same type of violence and threats online.
- My work becomes impossible without safe access to online spaces.

6. After participants have arranged themselves following a statement, ask 2-3 participants why they chose to stand where they are, as this can make for interesting discussions.

7. You can also tell participants that if, after hearing someone's explanation, they decide that they've changed their opinion, they can move to a different spot on the spectrum if they want – be sure to ask why they decided to move!

A feminist internet

- **Objective(s):** To provide an awareness raising opportunity for participants about the challenges faced by women in online spaces.
- **Length:** 40 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Her-story of technology[1]
  - Symbolic violence[2]
- **Needed materials:**
  - Flipchart paper
  - Colored Markers
  - Copies of Feminist Principles of the Internet[3] for participants

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

[2] https://cyber-women.com/en/online-violence-against-women/symbolic-violence/

[3] http://feministinternet.net

Leading the session

Part 1 – Raising Awareness

1. Start the session by asking participants - What some common messages or ideas they have heard about women and technology? What are the prevailing attitudes regarding women and technology in their country(ies)?
2. Ask participants to brainstorm some of the obstacles that women often face while trying to access and use technology, or participate actively in online spaces. They can do this all together, or in small groups – the choice is yours. Write down the obstacles that the group comes up with on a large sheet of flipchart paper.
3. Once the brainstorming and discussion has completed, share some of the following global statistics with participants - if possible, also try to include specific country or region-focused statistics relevant to the context of participants:

- Internet penetration rates are higher for men than for women in all regions of the world - the global Internet user gender gap is 12%.
- 60% of the cases of technology-related violence against women were not investigated by authorities.
- Of all the Wikipedia editors online globally, between 84 and 91% percent of them are male.
- Women occupy 27% of the top management jobs in media companies and 35% of the workforce in newsrooms.
- Women in tech are paid at least 28 percent less than men with the same education, years of experience and age.

4. Divide participants into small groups and ask them to reflect on the data shared - What are the implications of these statistics for the lives of women, and for shaping the Internet as a common space for all of us to inhabit freely?

Part 2 - Feminist Principles of the Internet

5. Now introduce APC's Feminist Principles of Internet, as an exercise to reflect on what is needed to build:

...a feminist internet that works towards empowering more women and queer persons to fully enjoy our rights, engage in pleasure and play, and dismantle patriarchy.

6. Give each of the groups a set of the Feminist Principles of the Internet – this can be the actual document itself (downloaded from the site) or a handout with the text of the principles, which are divided into the categories of:

- Access
- Movements and Public Participation
- Economy
- Expression
- Agency

7. Ask each group to discuss how each of the principles applies to their own context, and to make a list of ways in which each participant can contribute to changing that reality of women and technology.

8. Ask each group to present the principles they reflected on and their conclusions.

References

- http://feministinternet.net
- https://en.wikipedia.org/wiki/Gender_bias_on_Wikipedia
- http://cdn.agilitycms.com/who-makes-the-news/Imported/reports_2015/global/gmmp_global_report_en.pdf

Symbolic violence

- **Objective(s):** Demonstrate for participants how to identify symbolic violence, and how to draw connections between symbolic violence and online gender-based violence.
- **Length:** 30-45 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Spectrogram[1]
  - A feminist internet[2]
- **Needed materials:**
  - Flip charts
  - Pens or pencils
  - Colored sheets
  - Post-It Notes
  - Adhesive Tape

[1]https://cyber-women.com/en/online-violence-against-women/spectrogram/
[2]https://cyber-women.com/en/online-violence-against-women/a-feminist-internet/

Leading the exercise

Part 1 - What is Symbolic Violence?

1. Begin with an explanation of what is meant by the term 'symbolic violence':

   Symbolic violence is inflicted through impositions of gendered cultural norms and behaviors. Women are taught that "something" might happen to us if we decide to walk alone at night, dress a certain way, or act carelessly: fear becomes a normalized and accepted mental state.

   This means that we, as women, are held responsible for any violence we might face, which in turn creates fear or even terror – this fear or terror generates a "mental map of forbidden spaces" for us, eliciting conditioned responses such as:

   Feeling the need to return home at night in a taxi or with a companion; Walking more quickly or even running if we hear footsteps behind us; Unconsciously practicing self-censorship on social media and other online platforms; Deciding not to go out, or to dress a certain way, for fear of what may happen to us;

   Furthermore, though women are made to feel responsible for the violence we experience, at the same time we are never provided strategies and resources to address that violence (aside from the conditioned responses above), nor to enjoy and occupy spaces, or to be free in our movement and speech and with our body and sexualities, etc.

   Symbolic violence creates prohibited spaces and situations for women, thereby denying us our fundamental right to security and free movement; compounding this problem is the impunity often granted to our aggressors – often, they are not questioned but rather pathologized as "crazy" or inherently unable to take control of or responsibility for their actions.

   At this point, you may also want to discuss images of violence

against women (symbolic or otherwise) which are disseminated and normalized through the media, and especially in online spaces.

Part 2 - Identifying Symbolic Violence for Ourselves

2. Hand out to each participant a small stack of post-it notes, on which they should identify and write down examples of activities they have stopped doing, or behaviors they have modified, because of the symbolic violence they experience as women occupying offline and online spaces. Once finished, gather the post-its and read aloud some of the examples shared – discuss these together as a group, commenting on possible motivations for changing these behaviors and perceived fears.

3. Immediately following the group discussion, explain that there are three main factors which construct and enable fear and terror in response to symbolic violence:

- **Appropriation of the Female Body:** the female body is still seen as an object for male enjoyment, bring about a lack of security or confidence in the body's own resources and capacities.

- **Guilt and Shame:** these are both seen as permanent, unshakeable elements that facilitate the perception of perpetrated gender-based violence as deserved or somehow acceptable.

- **"Learned Helplessness":** this is a psychological state that occurs frequently when events are seen to be uncontrollable – when the perception is that there is nothing that can be done to change the outcome of an action, the mental state adjusts accordingly by sacrificing its agency to assert any control over that outcome (instead, accepting and normalizing it).

5. After explaining these three factors, ask participants what strategies they can think of to transform these factors into approaches for tackling symbolic violence! Have them write these down on their post-it notes. Below are some possible strategies that could be proposed:

- Regaining control of your body's narrative, defining and asserting it as a territory of both pleasure and resistance.
- Recognize and accept the damage which has been done to your body (physically or mentally), moving past any self-perception as a victim and instead building up the resilience of a survivor.
- Build and sustain networks of support for yourself and others, both online and offline. We are never alone in this struggle.

References

- https://en.wikipedia.org/wiki/Learned_helplessness
- http://www.autodefensafeminista.com/attachments/article/277/MANUAL%20Autodefensa%20Feminista.pdf

Reporting abuse on social media platforms

- **Objective(s):** To share with participants some tips for denouncing online violence in social media platforms like facebook and twitter.
- **Length:** 40 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Safe online campaigning[1]
  - Apps and online platforms: friend or foe?[2]
  - Let's start a documentation journal![3]
- **Needed materials:**
  - Projector and slides
  - Post its
  - Computer for every two participants (if possible)
- **Recommendations:** This session is highly recommended for groups

[1] https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/

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

[3] https://cyber-women.com/en/online-violence-against-women/lets-start-a-documentation-journal/

of women who have being harassed online or who are involved in online campaigning.

Leading the session

1. Start the session by asking participants:

- Do they know of any women's collectives or women activists who have been harassed online?
- If so, on which platform(s) did it happened?

Ask them to offer examples of tactics they have seen used by those groups or individuals to address or counter online harassment, or tactics that they themselves have used. Have participants write these on post-it notes.

2. Share some recommendations of basic practices for denouncing online violence against women that are commonly used, as well as any NGOs or collectives that can provide assistance in response to such harassment:

- Facebook recommends flagging the exact comment or post, providing as much context as possible in the reporting process. Participants can check updates to this process here: https://www.facebook.com/report
- Blocking harassers will prevent them from sending friend/follow requests, starting a conversation or sending any messages, and seeing any updates posted to a user's feed. Users are not notified when they've been blocked, but they may still notice that it has happened if they are suddenly no longer able to contact a target.
- Take screenshots before blocking harassers on platforms to keep as documented evidence of abuse – once they are blocked, it becomes much more difficult to collect supporting evidence, which users may be asked to offer during an investigation into the incident (you may want to show participants how to take screenshots on their computers if they don't know to do so already)

- Twitter recommends that users who are the target of online harassment report the incident and keep a record of the case number for any follow up action. On Twitter it is possible to report an individual tweet as well as an entire profile.

It is recommended to avoid clicking on any links that may be received in messages or other communication sent by harassers, as they could potentially lead to malware being installed on a user's device.

3. During this part of the session, you should also demonstrate to participants how they can block users and report profiles or posts on Facebook and Twitter, in addition to any other social media platforms that they frequently use. Make sure to research these before the training so you are up to date, as these processes unfortunately tend to change quite frequently (as do account privacy settings).

4. If you would like to offer participants an opportunity for some hands-on practice, have them break off into small groups and look for pages or profiles that may be targets of online abuse or harassment - for example, they should try out documenting any posts or profiles on Facebook that are actively perpetrating such harassment, and then filing reports using the established process.

References

- https://karisma.org.co/descargar/manualseguridadtw

Let's start a documentation journal!

- **Objective(s):** To introduce participants to more in-depth practices related to reporting abuse online, specifically documentation of incidents.
- **Length:** 45 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Reporting abuse on social media platforms[1]
  - Doxxing the troll[2]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
  - Printed copies of Documentation Journal templates (see below)
- **Recommendations:** This session is recommended when working

[1] https://cyber-women.com/en/online-violence-against-women/reporting-abuse-on-social-media-platforms/

[2] https://cyber-women.com/en/online-violence-against-women/doxxing-the-troll/

with groups that deal with online harassment, those who have received threats online and offline, or those who will be working on projects or campaigns that could elevate their risk of exposure to harassment.

Leading the session

Part 1 - Why is Documentation Important?

1. In this first part of the session, you will begin by explaining the following to participants:

   What is Documentation?

   Documentation in this context refers to a systematic, organized approach for keeping a track of any incidents of abuse or harassment that occur in the course of our work – essentially, it is maintaining an archive of evidence.

   What is an Incident?

   An incident is anything that happens either online or offline that might constitute abuse or harassment – whether an event can be classified as an incident or not is highly dependent on the context and circumstances in which it happens, and the severity of its impact in relation to those. For example, if you receive an email that seems like a phishing attempt – and you're used to receiving these every so often – that alone might not be significant enough to be an incident; however, if your organization is about to launch a major campaign, and you begin receiving an unusually large number of these emails, this would likely constitute an incident (and it should be documented). To provide another example, the same could be said if your organization is about to launch a major campaign and you begin receiving usually large numbers of Facebook friend requests from strangers.

   What is a Documentation Journal?

A documentation journal is a place where you can keep records of incidents that occur, in an organized way that will help you save important information and evidence from each for later use or reference.

Why is Documentation Important?

Documentation can be useful for later reference when attempting to connect the dots between different incidents that took place during a specific timeframe, or that happened to several people in the same organization. Documentation can reveal patterns of abuse or other online attacks you may not have otherwise noticed, by presenting a collated body of evidence – these patterns can be helpful for identifying adversaries, or to draw connections between certain kinds of incidents and certain actions of yours or your organizations. When reporting incidents of abuse on social media platforms, for instance, evidence such as screenshots or profile names may be requested during an investigation.

Part 2 – How Can We Document Incidents?

2. Once you've finished reviewing the above points about documentation and why it is important, you can hand out to participants printed copies of the below Documentation Journal templates.
3. Mention to participants that these templates provide just one example of the kinds of information that could be important to gather when documenting incidents. They should feel free to add or remove columns and fields as they see fit when creating more specific formats contextualized to their work in the future.

There are two templates included here – one for documenting online incidents, and another for physical/offline incidents (begins next page):

Documentation Journal Template (Online)

_____

Date

Time

Summary of incident

Platform

URL

Screenshot (filename or copy/pasted)

Description of screenshot content(s)

Risk level

Follow-up actions

Notes

Documentation Journal Template (Offline/Physical)

Date

Time

Location

Summary of incident

People involved

Risk level

Follow-up actions

Notes

4. Most of the fields in these templates are relatively self-explanatory; however, you should still walkthrough each one for the group, describing briefly to what each one refers (in terms of what participants should be keeping track of for each).

5. Be sure to specifically highlight the **Level of Risk** field, as this field is highly subjective and less self-explanatory than the others. How different participants and/or organizations define levels of risk will be extremely specific to their context – it might be useful to pause at this point and ask participants for examples of incidents they would define as Low Risk, Medium Risk, or High Risk (for instance). Emphasize to participants that they should consider the potential **impact** of the incident (on either a personal or organizational level, or both) when defining risk in this context.

   Optional: Either before or immediately following this session, go through the Gender-Based Risk Model exercise with participants. During that exercise, the group will have a more focused opportunity to define levels of risk for their own context – they can then apply those definitions of risk to their documentation journals.

6. Finally, another important field to highlight during this part of the session is **Follow-up Actions**. Essentially, a Follow-up Action is the next step that will be taken to address the current incident (such as filing a report on Facebook), or a measure that will be implemented to prevent the incident from happening again or to reduce its impact.

   Optional: Either before or immediately following this session, go through the Organizational Security Plans and Protocols session with participants. During that exercise, the group will have a more focused opportunity to define security plans and protocols in response to certain known or potential risks – similar steps would be required when planning Follow-up Actions for incidents.

Part 3 – Starting Our Documentation Journals

7. Ask participants to begin filling in their journal templates individually - give 10-15 minutes to fill in as much as they can. Although they can fill in the details of actual incidents that have occurred if they wish, participants can also use hypothetical examples for practice purposes.

8. Once they finish their first draft of the journal, ask them to get together in pairs and share the incidents they've recorded with their partner – for this step, pairing together participants from the same organization (if applicable) will be helpful. Each pair should ask questions of each other about the level of detail or thoroughness in their incident reports – in some cases, this may help a participant recall specific details they may not have remembered earlier. Note that **some participants might not feel comfortable sharing their journal with others**, so allow them to work individually if they so choose.

Part 4 - Practices and Tips for Maintaining Documentation Journals

9. Remind participants that, to keep up regular maintenance of their documentation journals, they will need to find ways to "socialize" (or integrate) journal updating into existing routines. In the context of an organization, participants should think about whether there will be a specific person in charge of gathering information for the journal; alternatively, it may be easier or more agreeable to rotate the task among individuals or among teams. You should also mention here that it may be good idea, if someone within the organization is the subject of an incident, for someone other than themselves to document the incident.

10. Encourage participants to experiment with different workflows to make updating their documentation journals a more efficient process – there may be ways of automating certain processes, or they may find that certain fields in the templates included above are irrelevant for their context (which will save them unnecessary work.

11. Close the session by asking participants, now that they've had time to think about the importance of documenting incidents for their own contexts, if they have any key takeaways from the discussion or ideas to make journal maintenance and updating an easier process.

Doxxing the troll

- **Objective(s):** To introduce participants into a series of tools and activities focused on gathering information about their online harassers. this information can be used to help them make decisions in terms of privacy and security online.
- **Length:** 180 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
  - Safe browsing[1]
  - What does your metadata say about you?[2]
- **Related sessions/exercises:**
  - Safe browsing[3]
  - What does your metadata say about you?[4]
  - Let's start a documentation journal![5]
- **Needed materials:**

[1] https://cyber-women.com/en/digital-security-basics-1/safe-browsing/

[2] https://cyber-women.com/en/safe-online-advocacy/what-does-your-metadata-say-about-you/

[3] https://cyber-women.com/en/digital-security-basics-1/safe-browsing/

[4] https://cyber-women.com/en/safe-online-advocacy/what-does-your-metadata-say-about-you/

[5] https://cyber-women.com/en/online-violence-against-women/lets-start-a-documentation-journal/

  - Printed copies of the Documentation Journal Template (Online)
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
- **Recommendations:** This exercise is recommended for groups of whrds that are currently experiencing online harassment/online threats, or those who have very recently experienced these. though not explicitly required, this exercise works best if participants have already done let's start a documentation journal! this exercise works best if participants each have their own device or computer. you may want to split this session into two parts, as it is quite long and can be very intensive – you can also keep this as one session, but with a longer than normal break in the middle.

This exercise was adapted from an activity developed by Indira Cornelio (SocialTIC) and Phi Requiem (#SeguridadDigital) with the collaboration and support of APC's Take Back the Tech

Leading the exercise

Part 1 – What is Doxxing?

1. Explain to participants what Doxxing means – essentially, it's the practice of gathering a substantial amount of personal information about someone and then making it public (usually online). You should also explain how doxxing is sometimes used against people as a revenge tactic, and is often used to endanger, harass, or threaten activists and human rights defenders.

2. Highlight this important reminder for participants before continuing onward with the exercise:

   The goal of this exercise is not to recommend doxxing as a best practice (or to recommend using illegal or dubious methods of doing so) – as doxxing implies the public release of personal information, it is important to highlight that 'outing' someone's identity or information is not necessary. Rather, the goal of this session is to show par-

ticipants how to gather this kind of information online to help them make informed decisions about addressing abuse or harassment.

3. Finally, explain also that it is important for participants to recall what they know about safe browsing practices – part of this exercise involved visiting harasser's profiles and online spaces.

Part 2 – Identifying Harassers

4. Work with participants to set their expectations for the exercise, asking them - What do they want to find out about their harasser(s)? Mention several possible motives before participants begin sharing:
    - Is it to know their real identity?
    - To understand their motives for harassing them?
    - To find out if they are harassing other WHRDs as well?
    - To find out if it is just one person, or several people acting as one?
5. You may find that some participants have heard of ways to obtain this kind of information about their harassers, but make it clear to them that the tools and tactics you will be sharing have certain limitations. If the group has already done the Let's Start a Documentation Journal! session, remind them of the importance of maintaining that body of evidence – it is critical for establishing patterns of abuse and for reporting harassment. If the group has not already done the Let's Start a Documentation Journal! session, explain that later in this exercise you will review a method for keeping track of harassment incidents.

Part 3 - Different Profiles, Different Motives

6. Share a couple of cases of women activists or journalists and their experiences with online harassment. Try to find cases that are relevant to the context of the participants, and that show different profiles of harassers and different motives for their actions.

7. Only if there are any women who feel comfortable sharing their own experiences with online harassment, ask them – About when did it begin? Who do they think the harasser is? Do they know them? Is there a specific motivation they can think of for their actions?

8. Reflect on possible motives that their harasser might have - Is the harassment happening because they are a women? Because they defend women's rights/human rights? Have they seen this kind of harassment against their male partners or colleagues? If so, does it happen the same way or differently?

Part 4 - Documenting Incidents & Threats

9. If participants have already gone through the Let's Start a Documentation Journal! session, review the key takeaways with participants once more and explain how a documentation practice is an important part of gathering information about harassers to make decisions about next steps and actions. You can then skip down to Part 5 – Getting Ready.

10. If participants have not yet gone through the Let's Start a Documentation Journal! session, start out by first explaining the following points, which highlight why documentation is an important practice for addressing online harassment:

    What is Documentation?

    Documentation in this context refers to a systematic, organized approach for keeping a track of any incidents of abuse or harassment that occur in the course of our work – essentially, it is maintaining an archive of evidence.

    What is an Incident?

    An incident is anything that happens either online or offline that might constitute abuse or harassment – whether an event can be classified as an incident or not is highly dependent on the context and circumstances in which it happens, and the severity of its impact in relation to those. For example, if you receive an email that seems like a phishing attempt – and you're used to receiving these

every so often – that alone might not be significant enough to be an incident; however, if your organization is about to launch a major campaign, and you begin receiving an unusually large number of these emails, this would likely constitute an incident (and it should be documented). To provide another example, the same could be said if your organization is about to launch a major campaign and you begin receiving usually large numbers of Facebook friend requests from strangers.

What is a Documentation Journal?

A documentation journal is a place where you can keep records of incidents that occur, in an organized way that will help you save important information and evidence from each for later use or reference.

Why is Documentation Important?

Documentation can be useful for later reference when attempting to connect the dots between different incidents that took place during a specific timeframe, or that happened to several people in the same organization. Documentation can reveal patterns of abuse or other online attacks you may not have otherwise noticed, by presenting a collated body of evidence – these patterns can be helpful for identifying adversaries, or to draw connections between certain kinds of incidents and certain actions of yours or your organizations. When reporting incidents of abuse on social media platforms, for instance, evidence such as screenshots or profile names may be requested during an investigation.

11. Now, you can introduce the Documentation Journal to participants – for this exercise, you can just use the Online version, which you should have printed versions of prepared to hand out to the group – see the template below:

Documentation Journal Template (Online)

Date

Time

Summary of incident

Platform

URL

Screenshot (filename or copy/pasted)

Description of screenshot content(s)

Risk level

Follow-up actions

Notes

12. Mention to participants that this template provides just one example of the kinds of information that could be important to gather when gathering information about harassers. They should feel free to add or remove columns and fields as they see fit when creating more specific formats that are relevant to their context.
13. Most of the fields in these templates are relatively self-explanatory; however, you should still walkthrough each one for the group, describing briefly to what each one refers (in terms of what participants should be keeping track of for each).
14. Be sure to specifically highlight the Level of Risk field, as this field is highly subjective and less self-explanatory than the others. How different participants and/or organizations define levels of risk will be extremely specific to their context – it might be useful to pause at this point and ask participants for examples of incidents they would define as Low Risk, Medium Risk, or High Risk (for instance). Emphasize to participants that they should consider the potential impact of the incident (on either a personal or organizational level, or both)

when defining risk in this context.

15. Ask participants to begin filling in their journal templates individually - give 10-15 minutes to fill in as much as they can. Although they can fill in the details of actual incidents that have occurred if they wish, participants can also use hypothetical examples for practice purposes.

Part 5 – Getting Ready

16. Before moving on to the next steps in the exercise, for participants to be careful not to click on any link they might receive or find while doxxing their harasser – these could be possible phishing attempts (explain what this is if participants are not familiar) that could install malicious software on their devices. Highlight that its extremely important to avoid providing additional information about yourself to harassers; likewise, for participants going through this exercise who are not currently experiencing online harassment, they will want to avoid attracting unnecessary attention to themselves that could lead to later harassment:

17. Walk participants through the following steps to safely begin gathering information about their harassers:

    - They should collect any information they may already have on hand about their harassers (or document any past incidents they can recall in their documentation journals);
    - Then, they should choose the browser they will use for their investigation – on that browser, they should logout from any of their accounts, and erase their browsing history and cookies. They may want to consider using Tor Browser for this activity, if you have already covered this with them;
    - They may also want to consider creating new online identities or profiles to perform this activity (such as an alias Facebook or Twitter account, or a fake Gmail account) – remind them to be careful not to use any information for these accounts that could be used to link back to their real identities!

- Emphasize the importance of taking notes during this process – remind the group of what you discussed when addressing the importance of documentation practices.
- Have participants create a dedicated folder on their computers to gather and store any information or evidence they collect – these could be avatar images, screenshots, user names, email and social media accounts, comments on forums, or mentions of their possible locations or other known contacts.

Part 7 – Useful Tools

18. Now you can start sharing examples of tools that will be useful to participants during their doxxing investigation - if possible, provide participants a copy of your presentation containing this information, or a handout with the tool list and links that they can refer to later on their own.
19. Explain each of the tools, giving participants a few minutes for each to locate them online and try them out (aside from those included here, feel free to add any others you know of that could be useful or relevant):
    - Google searching, or Duck Duck Go[6];
    - Advanced search on Twitter[7];
    - Checking Whois.net in case they can find information that comes from a website to see if there is any information about who owns the domain;
    - Google reverse image search[8] in case they have received images or photos they can do an image search;
    - Metadata tools in case they have received images or photos they can see if there is any metadata available:

[6] https://duckduckgo.com
[7] https://twitter.com/search-advanced
[8] https://images.google.com/

- MetaShield[9]
- MetaPicz[10]
- Social Mention[11];
- Follower Wonk[12];
- NameCheck[13];

20. Explain also that there are ways for participants to build mini-monitoring systems for tracking information online: this works well for tracking certain profile name, username or hashtag:

    - IFTTT[14] – for IFTTT, explain how it allows users to connect Twitter with Google Drive to keep track of tweets and mentions connected to a certain username or hashtag.
    - Google Alerts[15]
    - Tweetdeck[16]

21. Depending on how much time you have available, participants can either do their investigations now during the workshop, or they can do them as "homework" for the next training day. Either way, remind the group that it will be helpful – once they are done collecting information – to take a step back and look at everything they have gathered:

    - Do they see any patterns emerging?
    - What does the information they have tell them about who their harasser might be?
    - Perhaps they can even predict potential future targets or kinds of attacks?

[9] https://www.elevenpaths.com/technology/metashield/index.html
[10] http://metapicz.com/
[11] http://socialmention.com
[12] https://moz.com/followerwonk/
[13] https://namechk.com
[14] https://ifttt.com
[15] https://www.google.com/alerts
[16] https://tweetdeck.twitter.com

References

- https://summit2015.globalvoices.org/2015/02/do-we-feed-the-trolls-learning-from-our-community/
- https://citizenevidence.org/category/how-to-2/tutorials/

Part XII

Sexting

Time to watch!

- **Objective(s):** To introduce the practice of 'sexting' from a gender perspective, with an emphasis on how violence is still violence regardless of whether it happens online or offline.
- **Length:** 15 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - None
- **Needed materials:**
  - Laptop/computer and projector
  - Speakers (for video)

Leading the exercise

Go to https://vimeo.com/cyberwomen/1 and select the video "Case 1" – play this for the participants. Once the video has finished, discuss with participants what they saw - what do they think about the situation? What would they do?

Sexting

- **Objective(s):** Continue the discussion about sexting from a gender perspective from the previous session in this module (time to watch!), building on it to begin suggesting and recommending practices and tools for safer sexting.
- **Length:** 40 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Time to watch![1]
  - What does your metadata say about you?[2]
  - Anonymity[3]
  - Introduction to encryption[4]
- **Related sessions/exercises:**
  - Your rights, your technology[5]
  - Time to watch![6]

[1] https://cyber-women.com/en/sexting/time-to-watch/

[2] https://cyber-women.com/en/safe-online-advocacy/what-does-your-metadata-say-about-you/

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

[4] https://cyber-women.com/en/encryption/introduction-to-encryption/

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

[6] https://cyber-women.com/en/sexting/time-to-watch/

  - What does your metadata say about you?[7]
  - Anonymity[8]
  - Introduction to encryption[9]
- **Needed materials:**
  - Slides (with key points from below, and examples of anti-sexting campaigns)
  - Laptop/Computer and Projector setup
  - Speakers

Leading the session

Part 1 - Unpacking Social Stigma!

1. Start the session by showing some of the example anti-sexting campaigns - these can be videos or posters/advertisements with underlying narratives like “preventing sexting” or “why sexting is bad”.
2. Once you’ve demonstrated a few of these campaigns, split participants up into small groups of 3-4 people to analyze the campaigns. Give groups between 5-10 minutes for this discussion:
   - What is wrong with these campaigns?
   - How do they portray women?
   - Some campaigns even criminalize sexting, as well as the women who practice it – does this approach present a real solution to the real problem?

Part 2 - What is Sexting?

3. Once the small group discussions are complete, review with participants what sexting is; in your explanation, be sure to reinforce these points:

[7] https://cyber-women.com/en/safe-online-advocacy/what-does-your-metadata-say-about-you/
[8] https://cyber-women.com/en/anonymity/anonymity/
[9] https://cyber-women.com/en/encryption/introduction-to-encryption/

- The practice of taking and sending selfies and nudes can be an exercise of self-determination.
- Sexting can also be an act of pleasurable resistance against racism, sexism, machismo, conservatism and heteronormativity.

Ultimately, whether or not you share these kinds of pictures of yourself must be a choice that is exclusively yours, and must be a conscious exercise of both your right to self-expression and your right to privacy.

Part 3 – Safer Sexting?

4. In this part of the session, you can begin to offer some specific recommendations on practices that participants can implement for safer sexting. It's important to remember that there are different attitudes about identity and anonymity when it comes to sexting: some may feel more comfortable sexting with people they don't know, and others may feel safer sexting only with those individuals they know well.

   It is important here to be open to every possibility - provide digital security advice or recommendations based on specific preferences or doubts shared by participants, using some of the following suggestions as examples:

   - Play it safe - delete nudes or selfies that you send to others from your device as soon as you send them. When sending photos, do so over safer or secure channels (such as Signal – see more details below under Step 5).
   - Build rules or agreements with your sexting partners about not sharing your photos (or if sharing is okay, make agreements concerning with whom and how), what kind of detail your photos can contain, how you will send each other photos, etc.
   - Use a dedicated channel or app for sexting – while asking a sexting partner to download a new app or follow a specific procedure might not be the "sexiest" way to start things off, it's better than accidentally sending a photo of yourself over your regular SMS app to someone you didn't mean to send to!

- Be creative - look for your safest and sexiest angles in your photos!

5. If you will not already covered the session What Does Your Metadata Say About You? (or you will not have time to do so during this training) take about 15 minutes during this session to explain what metadata is and share a few examples – you can refer to that session for some examples.

   Explain that metadata in images can often provide identifying information about users, which is important to be aware of – in particular if sending nude selfies, and especially if the goal is to remain anonymous:

   To preserve anonymity, avoid showing any element(s) in a photo that could potentially identify you: these range from the more obvious (face, username) to more minute details (tattoos, furniture or belongings in the background, certain clothing), and finally to digital traces (photo metadata, geotagging, device information).

6. Finally, you may close the session out by making some recommendations on specific tools that participants use for safer sexting with partners:

   ObscuraCam: this mobile app produced by the Guardian Project allows users to "scrub" (remove) specific metadata details from their photos.

   Meet.jitsi: this browser-based platform offers HTTPS encryption and allows users to create temporary, one-time use chatrooms for video/audio chatting.

   Signal or Telegram: these mobile messaging apps offer varying levels of encrypted protection (of data while in transit between users) as well as user verification; in particular, Signal allows users to set "expiration" limits on messages or other content that they send (for example, after 5 minutes a photo can be set to disappear from the recipient's view of the conversation on their device).

References

- http://www.codingrights.org/wp-content/uploads/2015/11/zine_ingles_lado1.pdf
- http://www.codingrights.org/wp-content/uploads/2015/11/zine_ingles_lado2.pdf
- http://seguridadigital.org/post/148199830243/sextea-con-seguridad-diagrama
- http://lucysombra.org/TXT/Fanzine_necesito_privacidad.pdf
- https://guardianproject.info/apps/obscuracam
- https://meet.jit.si
- https://signal.org
- https://telegram.org
- https://acoso.online

Part XIII

Determining the best solution

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![1]
  - Organizational security plans and protocols[2]
- **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 3 towards the end after you've covered more specific tools

[1] https://cyber-women.com/en/online-violence-against-women/lets-start-a-documentation-journal/

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

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 be-

come 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:

Digital risk	Probability[3]
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 individual, 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

[3] 1=Very low; 5=Very high

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:

Digital risk:	Probability[4]	Impact[5]	Reaction[6]
Accidentally clicking an email link with malware!	4	3	3
Our offices are raided by the police to seize hard drives or other devices!	2	5	5

[4] 1=Very low; 5=Very high
[5] 1=Low severity; 5=High severity
[6] 1=Calm, under control; 5=Panicked, highly stressful

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:

Digital risk	Probability[7]	Impact[8]	Reaction[9]	What can I do?
Accidentally [...]	3	3		Download and install antivirus software; warn others in my network/organization in case they encounter the same link

Digital risk	Probability[7]	Impact[8]	Reaction[9]	What can I do?
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

[7] 1=Very low; 5=Very high
[8] 1=Low severity; 5=High severity
[9] 1=Calm, under control; 5=Panicked, highly stressful

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:**
  - Slides with key points included below
  - Laptop/computer and projector setup
  - Copies of WHRD case infographics (See Appendices)

[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/

- **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]
  - Apps and online platforms: friend or foe?[5]
  - Digital security decisions[6]

[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/

[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-

- **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.
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.

decisions/

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.

Part XIV

Privacy Policy

Content here

Part XV

Planning ahead

Organizational security plans and protocols

- **Objective(s):** To facilitate a process for women to develop a security plan and corresponding protocols that they can use to implement digital security measures in their own organization.
- **Length:** 90 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Hands-on practice with digital security tools and practices from previous training
  - Who do you trust?[1]
  - Gender-based risk model[2]
- **Related sessions/exercises:**
  - Personal perceptions of security[3]
  - Who do you trust?[4]

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

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

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

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

  - How does the internet work?[5]
  - Gender-based risk model[6]
  - Digital security plans and protocols: post-training replication[7]
- **Needed materials:**
  - Risk model from Gender-Based Risk Model exercise
  - Printed security protocol templates (see example template below)
- **Recommendations:** This session is best suited for participant groups who come from the same organization or collective, as the activities below are focused on developing an organizational level security plan – the process of designing this together will help support women's ongoing practice and implementation of it. it is crucial to follow-up with participants on the implementation of the plan they create – if possible, connect with them every two or three weeks to check on progress (apart from answering any questions they might send in the interim). be careful not to pressure participants about using specific tools or implementations of them when follow up with them – simply support them and be present with them, responding to any questions or concerns they have and providing recommendations when requested. if participants feel pressured, they may not be forthcoming about whether they've addressed a specific issue and won't feel comfortable sharing actual difficulties when they arise.

Leading the session

Part 1 – Return of the Risk Model

1. Begin the session by highlighting the importance of building a risk model before drafting a plan and any protocols. Remind participants that digital security is first and foremost a personal process - if their

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

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

[7] https://cyber-women.com/en/planning-ahead/digital-security-plans-and-protocols-post-training-replication/

goal is to draft and implement a digital security plan at an organizational level, explain that it will be a process of:

- Mapping threats collectively - this can be done over the course of a couple training sessions with the entire team present, however remind the group that remaining aware of and updated on the threats they face will be an ongoing process.
- Learning the difference between strong habits and unsafe habits of digital security, and remaining up to date on new tools or updates to existing ones.
- Making implementation decisions together as a team, but also identifying areas where individuals can create and practice their own processes as they see fit.
- Consistently monitoring the implementation of their organizational digital security plan, ensuring that corresponding protocols are well understood before they are practiced, and troubleshooting any emerging difficulties throughout.

Part 2 – Plans vs. Protocols

2. Explain to participants the difference between a digital security plan and a digital security protocol. The main idea to communicate is that:
    - A plan is an outline of key changes that an organization or collective has identified as requirements for increasing their digital security. Plans are a defined process, with a beginning and an end.
    - A protocol is a set of measures or actions related to digital security that are each connected to a specific activity or process within an organization or collective. Protocols are ongoing practices that remain in effect even when a digital security plan has been fully implemented, and will evolve over time in response to changes in risk and threat environments.

Provide examples of plans and protocols to participants – for instance, activities such as travel or participation in public protests would each have their own digital security protocol; items found in a digital security plan might include an organization having their website audited, verifying that every computer has antivirus installed, and introducing the use of GPG to encrypt emails.

Part 3 – Creating an Organizational Plan and Protocol

3. This session is best suited for participant groups who come from the same organization or collective, as they can take advantage of this opportunity to collaborative develop their plan and protocols as a team. However, if this is the case for only some participants, those who are not part of any organization or group can still participate in the session by working on their own personal plans and protocols.
4. Ask participants to refer to their risk model from the Gender-Based Risk Model exercise, as well as their notes from the Who Do You Trust? exercise. Have them begin making a draft of their security plan - the following format may be useful. Explain to participants each of the sections (a new row should be started for each risk or threat identified):

Threats and Risks	Which threats and risks do we currently face? Which could we potentially face in the future?
Identified Vulnerabilities	Which of our practices as individuals, or circumstances as an organization, could expose us to harm?
Strengths and Capacities	What strengths do we have as organization that give us an advantage in responding to identified threats and risks?
Mitigating Actions	What kind of measures do we need to take in order to mitigate the risks? To be better prepared for identified threats?

Resources Needed	What resources (economic, human, etc.) would we need to implement these actions?
Who Needs to be Involved?	Which areas or people within our organization need to be involved in implementation? Will any sign-off or other permissions be required?

5. Remind participants that although the focus of this training is on digital security, we must always remember to take holistic measures into account. Ask participants to consider which actions need to be taken in terms of physical security and self-care as they draft their security plans and protocols.
6. Then, after participants have finished their first draft of the plan template, ask them to then build a list of their organization's activities or processes that they feel will require individual protocols.
7. Once participants have finished both their draft plan template and their list of activities requiring security protocols, it will be useful to pause so that everyone can share their plans. This presents a valuable opportunity for participants to learn from the approaches of others; however, remember that some may not feel comfortable sharing their organizational or personal vulnerabilities as a matter of trust. To address this proactively, you may want to ask the group to share only the key items for their plan (the 4th column of the template table, "Mitigating Actions") while keeping other information like "Threats and Risks" and "Identified Vulnerabilities" private.

Part 4 – What's Next?

8. Discuss follow-up steps with participants - they will need to have a focused gathering within their organizations to share insights and key takeaways from this session, as well as the Gender-Based Risk Model exercise and the Who Do You Trust? exercise – of special importance from this session will be the list of activities and processes requiring security protocols. This plan will need to be discussed and agreed upon as a team, with realistic dates set for its im-

plementation – while considering these, participants also need to remember that there may be others in their organizations who will require training on digital security practices and/or specific tools for full implementation to be possible.

Digital security plans and protocols

- **Objective(s):** To build on the organizational security plans and protocols session. here, you will present a set of recommendations that can help participants facilitate post-training implementation of their security plans and protocols within their organizations.
- **Length:** 40 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Hands-on practice with digital security tools and practices from previous training
  - Organizational security plans and protocols[1]
  - Who do you trust?[2]
  - Gender-based risk model[3]
- **Related sessions/exercises:**
  - Organizational security plans and protocols[4]

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

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

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

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

  - Who do you trust?[5]
  - Gender-based risk model[6]
- **Needed materials:**
  - Slides with key points included below
  - Laptop/computer and projector setup

Leading the session

Part 1 – Mapping Organizational Structures and Barriers

1. Working in pairs, ask participants to describe their organizations:
   - How many people participate in them?
   - How often do they meet?
   - Are there areas or committees that bring different parts of the organization together?
2. Remaining in pairs, now ask participants to share with one another some of the barriers or challenges they anticipate facing within their organizations when presenting their security plans and articulating the need to begin an implementation process.

Part 2 – Facilitating Organizational Implementation

3. Once the groups have finished discussing the points above, share some ideas that can help participants facilitate post-training implementation of their security plans and protocols within their organizations:
   - Recommend that they frame this as the beginning of a reflection process - it will take time to get the plan implemented and the protocols developed and tested, and there will be an adjustment period as people get used to these changes. Regardless,

protocols/

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

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

they should make sure to emphasize that thinking in a more critical way about organizational security is a positive step.

- Warn participants that they might receive some push-back on the term "protocols" as it may come across as overly technical and intensive; they should remind others in their organizations that protocols are nothing more than an agreement about the specific risks and threats they face, and a commitment to solve them together by putting strategic actions into place for the good of the organization and its mission.
- Underscore the importance of collaboration and inclusion in the implementation process – participants should work with different teams within their organizations on their team-level risk assessments, and have them share the outcomes and next steps with the rest of their colleagues. Emphasize also that it will be critical for participants to hold space for others in their organization to provide feedback on the security plan and protocols – as different people's tasks will be affected in different ways by these new measures, they will want to avoid creating additional difficulty for anybody's work.
- Have participants consider other ways to collectively engage different teams across their organization – one such approach is for them to propose a "digital security commission" that includes representatives (who are empowered to make decisions) from each team or area who are together tasked with overseeing the implementation of the security plan. They can go about this process gradually, focusing first on high-level staff or starting out only with specific teams and then expanding outward. The approach that works best will vary widely by organization.
- Finally - ask the participants to share some of the ideas they have that could help facilitate the implementation process for their organizations.

Part 3 – Starting the Conversation

4. Share with participants a basic structure for starting this important conversation within their organizations - it could be a set of questions, or a possible training plan of their own with specific sessions and exercises relevant to the organizational risk context.

5. Remind the group to be aware of the logistics involved, time in particular – people within their organization may not have the time to set aside an entire afternoon, day or even longer for training. Changing long-standing habits takes a lot of time and patience, so it's will be more ideal for participants to find ways of building these conversations (or trainings) into existing regular meetings or other gatherings.

   Here is a basic structure that participants could follow to raise awareness of certain topics – this begins with a conversation about why digital security is important for the organization, and then includes sessions (from this curriculum) which go into further detail on basic digital security topics - how participants ultimately choose to have these conversations is up to them:

   - Conversation: Why Digital Security is Important for Our Organization
   - Session: How does the internet work?[7]
   - Session: Let's start a documentation journal![8]
   - Session: Mobile phones 1[9]
   - Session: Encrypted communication[10]
   - Session: Safe browsing[11]
   - Exercise: Gender-based risk model[12]

6. Remind participants that this is just a suggested approach – they should feel free to adjust the sessions and the topics as they see fit. It

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

[8] https://cyber-women.com/en/online-violence-against-women/lets-start-a-documentation-journal/

[9] https://cyber-women.com/en/safer-mobiles/mobile-phones-1/

[10] https://cyber-women.com/en/encryption/encrypted-communication/

[11] https://cyber-women.com/en/digital-security-basics-1/safe-browsing/

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

is important that, as participants work through the implementation process with their organizations, that you make yourself available (to the extent possible) to provide support and answer any question they might have.

Part XVI

Self-care

Building feminist self-care

- **Objective(s):** To give participants an opportunity to reflect on the importance of self-care in their daily lives, allowing them to build a definition of self-care in a judgement-free environment.
- **Length:** 30 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Personal perceptions of security[1]
  - Who do you trust?[2]
- **Needed materials:**
  - A rubber ball (or any small, throwable object)
- **Recommendations:** Self-care is an essential part of a holistic digital security practice, and is important to consistently reinforce and encourage – it is highly recommended that you distribute exercises from this module throughout your training. for this and all sessions in your training, always be conscious of and sensitive to women's different physical abilities and limitations. this exercise is best done near the start of the training, or at the beginning of an individ-

[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/

ual training day; as it is a very reflective and introspective exercise, make sure it is well spaced from other self-care related exercises.

This exercise was adapted from content in Mujeres Al Borde's Manual "Self-Care and Feminist Healing for Unmanageable"

Leading the exercise

1. Begin the exercise by introducing the idea of self-care – ask participants if they are familiar with the concept, or know what it is. Define the concept of self-care for the group, and explain that this exercise will be focus on self-care as a feminist practice in the context of WHRDs.
2. Now, explain how this (very simple) exercise works:

- Have participants get up and out of their seats, giving them all a few moments to stretch and move around – then, have everyone stand in a circle.
- You will begin by gently throwing a small ball (or other throwable object) to one of the participants.
- When they catch it, you will ask them a question eliciting their thoughts on aspects of self-care as it relates to them personally (you can use the examples included below).
- Once they have answered, the participant will throw the ball back to you; then, you will throw it to another participant, and repeat the process above. You can keep going until everyone has had the chance to answer a question.

Here are some example questions you can use for this exercise (feel free to also ask any other similar questions focused on self-care that you can think of):

- What is self-care for you? What is collective care? How are they different?
- Is self-care an issue addressed in your organizations, groups or collectives?

- Do you practice self-care? What are your self-care practices?
- Do you find it difficult to think of yourself as a person who deserves care?
- Do you find difficult to think in yourself as a person whom deserves care?
- As WHRDs, do you think our tendency is to focus more on taking care others at the expense of ourselves?
- Do you feel that you're aware of what your body and soul needs?

3. Once everybody has had the chance to answer a question, or otherwise express their thoughts or practices related to self-care, close the discussion by giving a quick summary of what was shared by the group – is this a group of women who are new to self-care as an intentional practice, and perhaps doesn't practice it very often (or at all)? Perhaps these are women who are already quite familiar with self-care, and practice it regularly? Or maybe it's a mix of women, some of whom are very familiar and others not so much, who can learn from each other? Highlight any insights or practices shared by the group – and make sure to positively emphasize anything they are already doing well!
4. Ask the group – are the responsibilities that we have as women human rights defenders different from those of our male counterparts? Discuss the social burdens they are expected to carry, especially the caretaker role - to take care of home and family, and sometimes even work and colleagues – that society often imposes on women.
5. Analyze how these additional responsibilities can impact their work as WHRDs, and how this compares to the challenges faced by men. Here, you could also raise the issue of the guilt often experienced by WHRDs – they must frequently decide between their activism and their personal lives and families, and feel that regardless of their choice, their choosing of one signifies a profound neglect of the other.
6. After these discussions, close the exercise by asking participants if they would like to propose any self-care practices for the training process; for example, this could mean beginning the training a bit

later each day, taking more frequent and shorter breaks, taking certain meals together, etc.

The loving touch

- **Objective(s):** Conectarse las unas con las otras a través del tacto y contacto corporal para reflexionar sobre cómo damos y recibimos amor, cariño y afecto.
- **Length:** 20-30 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - The rules of the game[1]
  - Building feminist self-care[2]
- **Needed materials:**
  - Mattresses or blankets
  - Cushions or pillows
  - Quiet, relaxing music
- **Recommendations:** Self-care is an essential part of a holistic digital security practice, and is important to consistently reinforce and encourage – it is highly recommended that you distribute exercises from this module throughout your training. for this and all sessions in your training, always be conscious of and sensitive to women's different physical abilities and limitations. both you and other par-

[1] https://cyber-women.com/en/trust-building-exercises/the-rules-of-the-game/
[2] https://cyber-women.com/en/self-care/building-feminist-self-care/

ticipants must remain aware of and sensitive to those women who may not be comfortable with being touched by others (this is especially true of certain cultures over others) – for this reason, this exercise is best for groups of women who already know and trust one another. if some women prefer not to participate in the activity, let them know that this is completely acceptable. reassure them that they will not be made to feel uncomfortable, and that they can still participate by lying down and taking a few minutes to relax with slow, deep breaths.

This exercise was adapted from content in the IM Defenders Self-Care Manual

Leading the exercise

1. Arrange the blankets, cushions and pillows in a circle on the floor - ask half of the group to lie down on their backs in the circle, with their heads towards the center as if forming the petals of a flower. Invite them to close their eyes and relax. Make sure there is at least one-person-width of space between each participant.
2. Ask the other half of participants get comfortable in the spaces between the other participants, each in a seated position next to the knees of those who are lying down.
3. You will lead this session using your voice. Explain to the seated group that they will give a "loving touch" to the women lying down next to them, touching and caressing them in a respectful way as you will soon describe. Those who are not comfortable touching others can place their hand on the head or shoulder of their partner, or simply close their eyes and listen to your voice.
4. In a calm, soothing tone of voice, you will give the seated women several instructions for their loving touches, with 2-3 minutes of spacing between each. Remind everybody that breath is very important for this exercise – they should all breathe slowly, inhaling through the nose and exhaling through the mouth:

- **First Instruction:** Caress the head of your partner.

- **Second Instruction:** Caress the forehead of your partner.
- **Third Instruction:** Caress the arms of your partner.
- **Fourth Instruction:** Caress the hands and fingers of your partner.

5. As the group progresses through the activity, talk about:

- As women activists and human rights defenders, we typically have very little time for ourselves. Those who are caressing their partners are allowing them a rare opportunity to relax and feel taken care of.
- The social burdens and responsibilities carried by women – as human rights defenders, mothers, sisters, we are always expected to take care of others, but do we take care of ourselves? Our lives often have very little space for self-care or collective care.

6. Once the women who are seated are done caressing the hands and fingers of their partner, give the women who are lying down a few moments to open their eyes and change positions with her partner. Repeat the process above, so that everyone who has given also has the chance to receive.

Look

- **Objective(s):** Women will push back on any feelings of monotony, disenchantment, sadness and disconnection by activating their desire to dream and rejoice with life.
- **Length:** 20 minutes (depends on group size)
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - The loving touch[1]
  - Building feminist self-care[2]
- **Needed materials:**
  - An open and relaxed mind
- **Recommendations:** Self-care is an essential part of a holistic digital security practice, and is important to consistently reinforce and encourage – it is highly recommended that you distribute exercises from this module throughout your training. for this and all sessions in your training, always be conscious of and sensitive to women's different physical abilities and limitations.

This exercise was adapted from content in Mujeres Al Borde's Manual

[1] https://cyber-women.com/en/self-care/the-loving-touch/
[2] https://cyber-women.com/en/self-care/building-feminist-self-care/

"Self-Care and Feminist Healing for Unmanageable"

Leading the exercise

1. Begin by explaining how, in the daily life of a woman activist or human rights defender, it can be easy to become overwhelmed by feelings of monotony, disenchantment, sadness and disconnection to overcome.
2. Continue by explaining that, during this exercise, participants will address those feelings they experience when they are struggling, or feel lost and without a sense of direction – they will do this by activating an energy point which, in traditional Eastern medicine, activates the desire to dream and to feel enchanted by life again.
3. Invite the participants to sit in a circle, either in their seats or on the floor.
4. Lead the group through the following steps (have them repeat this three times):

- Locate your energy point – it sits right between your eyes, just below your eyebrows and just above the bridge of your nose.
- Inhale with a deep, cleansing breath and hold it.
- With your thumb, press down on your energy point – as you exhale, think of something that inspires you and makes you feel alive.

5. Finalize the session by inviting participants to use this technique whenever they feel the need to center themselves and push back on feelings of despair or melancholy. Talk about how it is okay to feel afraid, tired or disenchanted at times, and how everybody has felt this was at one time or another.

Our reflection

- **Objective(s):** To give participants an opportunity to think about their own self-care practices – specifically, which ones they already do well, which ones they could improve, and which ones they might want to adopt.
- **Length:** 20-30 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - I decide[1]
  - The loving touch[2]
  - Building feminist self-care[3]
  - Look[4]
- **Needed materials:**
  - Mirrors for each participant
  - Dot stickers
  - Optional: Participants can use a photo of themselves instead of mirror (ask them to bring these ahead of time)

[1] https://cyber-women.com/en/determining-the-best-solution/i-decide/
[2] https://cyber-women.com/en/self-care/the-loving-touch/
[3] https://cyber-women.com/en/self-care/building-feminist-self-care/
[4] https://cyber-women.com/en/self-care/look/

- **Recommendations:** Self-care is an essential part of a holistic digital security practice, and is important to consistently reinforce and encourage – it is highly recommended that you distribute exercises from this module throughout your training. to create an environment that encourages relaxation and introspection, you may light some candles, burn some incense, or play some soft, soothing music during this exercise.

Leading the eExercise

1. Give each participant a small mirror, or if not using mirrors, ask them to take out their photos of themselves. Hand out the dot stickers.
2. Explain that you will read a series of statements, which participants should answer either "Yes" or "No" for themselves. For each time they answer "No" to a statement, they should place a dot sticker on the mirror or on their photo.
3. Below is a list of example statements that you can during this exercise; however, based on what you know about the group (and how comfortable the individual participants are with one another) you can add additional statements, or avoid certain ones:

- Every night, I get at least 8 hours of sleep and wake up feeling rested and ready to start the day;
- During the last six months / one year, I have had the option of taking a vacation available to me and have taken one;
- I have a healthy diet and make the effort to exercise regularly, to keep my body and mind in balance;
- I always find a little time for myself to read, to sleep, or to spend time with my friends and family;
- Whenever I get sick, I take days off to recover and concentrate on getting better, not on my work;

- Whenever I am overloaded, I always say no to offers of additional work;
- I get my semiannual gynecological exams as recommended;
- I take time to clarify and resolve misunderstandings with loved ones or work colleagues when any conflicts arise;
- I keep an 8-hour per day work schedule, which both myself and my organization respect;

4. When you finish with the questions, ask participants - What do they see in the mirror (or on their photos)? Bring the group together in a circle to discuss the effects that can excessive work burdens, poor social practices at work, or insufficient care for body and mind can have on individuals, blurring out their essence and obscuring who they really are at heart.
5. Go around the circle and ask whoever feels comfortable doing so to set an intention – that intention should be to begin taking better care of themselves by doing one of the self-care activities mentioned earlier more regularly.

The act of NO

- **Objective(s):** Reflection opportunity for women to think about on the burdens placed on them - as women, human rights defenders, or activists – and how they can better justify for themselves the need for self-care.
- **Length:** 10-15 minutes
- **Format:** Execise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - None
- **Needed materials:**
  - Honesty and Sensitivity
- **Recommendations:** Self-care is an essential part of a holistic digital security practice, and is important to consistently reinforce and encourage – it is highly recommended that you distribute exercises from this module throughout your training. some women may not feel comfortable telling their stories (see below), in which case they can instead tell the story of a friend, sister, or co-worker.

Leading the exercise

1. Introduce the exercise by talking with the group about the pressures that society often places on women – societal and cultural norms dictate that women must work two or three times as hard as men to prove their self-worth, for example.
2. Talk about how women human rights defenders face even more burdens – work overloads, self-guilt for failing to meet deadlines or accomplish goals, and being expected to take care of others' needs before their own are just a few examples.
3. Now, explain that with this exercise, participants will have an opportunity to reflect on the burdens they carry with them. Start by organizing the group into pairs.
4. Ask each pair to tell each other a story about a time they wanted to say NO, but didn't or couldn't – this could be a time they wanted to say no to extra work, or to a request for a favor, to spend time with a loved one or to fulfill another commitment. You can start by telling a story of your own, from a time when you wanted to say NO – for example:
    - I had planned a dinner with several friends, but while I was at work I was asked to stay late to resolve a problem that had arisen with an important project. I couldn't say NO, but I really, really wanted to.
5. Once each pair finishes, tell them that they will now re-tell their stories to each other; however, this time, they will change their stories as if they had actually said NO.
6. Tell participants that, if they wish, when they tell these alternative versions of their stories they can include how they would have explained (to their boss, colleague, or whoever was making the request of them) the reason why they are saying NO. This is not required, but it can be healthy reflection on the importance of making time for themselves.

Love letter to myself

- **Objective(s):** To provide space and time for women human right defenders to think about themselves, their concerns, and the actions they can take to relieve the pressures they face.
- **Length:** 20 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - None
- **Needed materials:**
  - Paper and Pens
  - Projector and laptop/computer (to show the sentences below)
  - Optional: if you would prefer not to have a projector for this session, you can write out the sentences below on a large piece of flipchart or poster board.
- **Recommendations:** Self-care is an essential part of a holistic digital security practice, and is important to consistently reinforce and encourage – it is highly recommended that you distribute exercises from this module throughout your training. depending on the group you are working with (and the amount of time you have for this exercise) consider closing this with a reflection on self-care and why it is important. ask participants - when was the last time they asked

themselves how they felt? is their activism having an impact in their health? how are they taking care of the most important resources they have for their activism work (themselves)?

Leading the exercise

1. On a prepared slide or sheet of flipchart paper, show participants the following:

   Dear .....,

   I have been watching you lately, I know you are having a difficult time with...

   I also know you are concerned about .....

   I just wanted to make sure you knew .....

   Remember you are great at .....

   I really think that you should .....

   And maybe try doing ..... in the coming weeks.

   Love, Yourself

2. Give one sheet of paper to each participant - ask them to fill in the blank space "Dear ....." with their name, and to complete the remaining sentences that were provided.
3. Remind participants that they will not have to share their letter with the rest of the group - this is a deeply personal activity.

Part XVII

Closing and review exercises

Witch coven

- **Objective(s):** To help raise participant energy levels and keep the group stimulated. it provides a welcome break from technical training content, while still connecting to digital security themes.
- **Length:** 10-15 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Her-story of technology[1]
- **Needed materials:**
  - Chairs (exactly one less than the number of participants)

Leading the exercise

1. Ask the group if they are familiar with the game "basket of fruits" (if not, "musical chairs" is another close reference) – explain that this game is a slightly feministified version.

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

2. Have the chairs arranged in a circle, and invite participants to have a seat – there should be one less chair than there are participants, so one person will remain standing.
3. Assign each participant with the name of an outstanding woman in the her-story of technology or feminism (your choice) – you can even use the same women that you covered together in the session Her-Story of Technology. Assign the same name to multiple participants.
4. Explain to the participants what a witch coven is – a night meeting of witches, where they tell stories and cast spells – and tell them that together you're going to have a witch coven of your own!
5. Start the coven by beginning a (made-up) story about some of the women in technology you're honoring:

- Each time you mention one of these women's names, the participants who have been assigned that name must quickly change their seats (the one participant who is standing gets to sit down).
- The participant who is left standing must now continue making up the rest of the story until they mention another name and participants change seats again.
- If at any point in the story the word "coven" is mentioned, this means that everyone must quickly get up and change seats.

6. Repeat the steps above several times until all the women's names have been called, or until everyone has had the chance to tell part of the story.

The cauldron

- **Objective(s):** To even out the participation playing field. in a group setting, some people tend to speak more than others - this exercise raises awareness of that fact, while inviting participants who have not spoken as much as others to do so.
- **Length:** 15-20 minutes (depends on group size)
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - None
- **Needed materials:**
  - Pre-cut slips of paper (3-5 per participant)
  - Bowl or basina
- **Recommendations:** The cauldron can be useful throughout your training – if introduced at the beginning of the workshop, you can use this exercise each time you ask the group a question during a session. that way, everyone has a chance to speak more often, and those who may be shy about answering questions are given the opportunity to get more comfortable. this exercise will revolve around a group discussion, which can be about anything; however, it works especially well if the discussion focuses on a topic from the training. you can introduce a new topic, or you can use this

exercise as a review for a previously discussed one – the choice is yours.

Leading the exercise

1. Have participants sit in a circle, arranged around the bowl or basin – this will be the cauldron. Give everyone 3-5 slips of paper.
2. Explain the rules for the discussion: every time someone speaks, they must throw one of their paper slips into the cauldron. Once a participant runs out of paper slips, they can no longer speak.
3. Introduce a topic, and facilitate the discussion by asking a series of questions to the group. For example, if the topic is malware and viruses, you might ask the following:

- What is malware?
- What are some different kinds of malware that you know of?
- Are there any operating systems that are immune to malware infection?
- Has your computer or smartphone ever been infected with malware? If yes, how did you know?
- What are some ways that we can protect our devices from malware infections?

4. Continue the discussion until everyone has run out of paper slips - you can reactivate the conversation if you wish, by moving on to a new topic and handing the paper slips back out to everyone.

Feminist flowers

- **Objective(s):** After an intensive day of digital security training (especially true of the first day or two) lead participants through this exercise to motivate and inspire them to keep going.
- **Length:** 10 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - None
- **Needed materials:**
  - Small slips of paper
  - Pen
  - SFlowers (real or paper/plastic)
- **Recommendations:** This exercise can be done multiple times throughout the training – you can end the first day or two in case you do not find natural flowers here you find a simple tutorial: https://www.youtube.com/watch?v=eunyko9wfae

Leading the exercise

1. Before beginning this exercise, you will need to do some preparation ahead of time:

Write short messages of encouragement on small slips of paper – here are a few examples:

- After this experience, I will not need a "technician" any longer.
- There is a community of women/feminists, and they have my back.
- I take a deep breath, and I reset my computer.
- I can do this - I've done much more difficult things before.
- My devices have no superpowers over me – I am in control.
- The only person who can decide how I practice digital security is me.

Once you're done writing these out, deposit each slip of paper inside one of the flowers.

2. Have the group sit in a circle, and ask them – How often do you feel frustrated or overwhelmed with technology? Remind everybody that this is totally normal, despite some of the challenges we face as women and human rights defenders.

3. Go around the circle and give each of the women one of the flowers – have them hold on to these, but ask that they not open them just yet.

4. Tell the group a story about a frustrating experience you've had as a trainer, or from when you first entered the digital security field. Tell them you can relate to their experiences with technology challenges, and remind them that there is nothing they cannot overcome by working together.

5. Now, ask participants to open their flowers – go around the circle and have each woman read aloud the message they find inside. Ask if they want to share any of their feelings or takeaways from the day, and if they want to share what their message means to them.

Magic circle

- **Objective(s):** To provide a closing, for a training process or individual session, in which participants set an intention to continue sharing with others what they have learned.
- **Length:** 30 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - None
- **Needed materials:**
  - Paper and Pen

Leading the exercise

1. New knowledge or experiences are made much richer shared and complemented with other people. Explain that the purpose of this exercise is for participants to set an intention to continue sharing with others what they have learned during the training process.
2. Invite the group to form a circle - they can be seated on the floor, in chairs, or standing, what is most comfortable for everyone.

3. As this exercise is called Magic Circle, begin the exercise by talking about some of the traditional symbolism and significance of the circle:

- Rituals have been celebrated and observed using circular arrangements since prehistory - it was believed that through the energy emanating between people in a circular pattern, evil spirits were exorcised and good spirits remained;
- In a circle, people are all visible to one another at equal distance – each person occupies the same level and plane as everybody else, and leadership is not disputed – it is trusted;
- Circles place the flow of energy in balance, with everybody giving as much as they receive; nobody comes first and nobody comes last – all become one and equal.

4. Invite participants to each write on a piece of paper something they are willing to share with the person to their right – this can be anything: a thought, a song, a poem, or something they learned during the training that is important to them. Once everybody has written something, ask them to fold their papers in half.

5. Each participant should have in their right hand the folded paper they wrote. Explain that the right hand symbolizes an individual's ability to help others, and the left hand symbolizes their need to exchange - everybody should now join hands in the circle, with each person's right hand joined with the left hand of the person to their right.

6. Everybody should now give their written message to the person on their right, passing it from their right hand into the left hand of the recipient.

7. Everyone should now read the paper they've received – they can either do this out loud, or quietly to themselves.

8. As they read their messages, speak to the group about the idea of sisterhood - the love between women in which all are perceived as equals and as allies, building solidarity from violence, inequality and injustices faced and changing each other's realities for the better.

Explain that together, you are all supporting each other in sisterhood by sharing knowledge and insight with one another.

Charades

- **Objective(s):** Trainings are often quite intensive, providing a lot of information to absorb in a relatively short time. this exercise is tool that you can use to test participants' knowledge and comprehension while simultaneously offering a fun and relaxing environment for de-stressing.
- **Length:** 15 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - None
- **Needed materials:**
  - Digital Safety Tool Figures[1]
  - Tape or clothespins
  - Music (to play in the background)
- **Recommendations:** In case some participants have trouble guessing their digital security tool figure, and others have already completed the exercise in their pairs, those who have finished can help others guess which figure they've been given.

[1] https://cyber-women.com/en/downloads/figures_fichas_adivinanzas_caja_herramientas.pdf

Leading the exercise

1. Have participants all stand in a line, with their backs facing you – using tape or a clothespin, fix one of the Digital Safety Tool Figures onto the back of each participant. Make sure that nobody sees which figure has been given to them!
2. Once finished, ask participants to arrange themselves in a large empty space in the room (or to create one by removing chairs or desks). Explain to them that the figure on each of their backs represents a concept or tool that they have discussed during the training.
3. Put on some music – participants should now move freely throughout the space. They can stretch out, dance, walk, or otherwise move about however they wish (but they must remain in motion). Explain that when you stop playing the music, everybody must also stop and remain in place.
4. Stop the music and ask each participant to partner with the person they find themselves closest to. One participant must show her back to the other person, who will then attempt to communicate – using only gestures or body expressions – the word or concept that is on their back. Once the participant guesses correctly, they will now switch places with their partner and repeat the process - the exercise ends once everyone has guessed correctly which digital security tool figure is on their back.

DigiSec rally

- **Objective(s):** To close out the training on an energizing note, you will lead participants through a dynamic grand rally adventure to review the digital safety knowledge they have learned.
- **Length:** 45 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - Varies, depending on what has been covered during the training.
- **Related sessions/exercises:**
  - Varies, depending on what has been covered during the training.
- **Needed materials:**
  - Large open air space, or indoor space with different rooms and corridors.
  - Pre-printed question sheets (one for each participant).
  - Pens and paper.
- **Recommendations:** The content of the cases you use for this rally will depend on the content that has been covered during the training – as this is meant to be a comprehensive review exercise, the rally is best done towards the very end of a training. the rally is also test for you as the trainer to identify where participants' strengths lie, and in which areas they may need further training or support.

the rally is designed to provide participants with a practical, hands-on opportunity to immediately apply what they've learned during the training – for this reason, the cases provided to participants for this exercise (example cases for you to use are included) should be focused on scenarios of direct incident response rather than recommending preventative measures.

Leading the exercise

Part 1 – Setting up the Rally Course

1. Before you begin, decide how many stations and cases your rally will have – for the purposes of demonstration, these instructions are based on a rally with five stations (one case each). Don't forget to include instructions in each case indicating to which station groups should proceed next upon solving it.
2. Distribute the five stations evenly throughout the space you have available, they can all be in the same room (or in different rooms if you have you have access) - this exercise works best if stations are in different spaces, as it makes the rally more dynamic and competitive. If possible, try to find location for the rally that is outside the training venue where you and the participants have been working – this will be provide a welcome change of scene.
3. Each of the stations will feature a case that participants must solve using what they've learned from the training, in addition to any toolkit you provide them (see below). The rally is best done in groups, with each group sent through the course via a different route so that the response time varies and to avoid overcrowding the stations.

Resource 1: Station Order and Team Route Guide

TEAM 1	TEAM 2
Station 1 (Start)	Station 5 (Start)
Station 2	Station 3
Station 3	Station 1
Station 4	Station 2
Station 5	Station 4
FINISH LINE	FINISH LINE

Resource 2: Case Toolkit

No.	Tool
1	Virtual Private Network (VPN)
2	Antivirus Software
3	Tor Browser & Anonymous Email Account
4	Encryption (PGP keys)
5	Security Protocol
6	Immediate Response Measures
7	Gender-Based Risk Model

Resource 3: Example Cases

CASE 1

> A filmmaker has just completed a documentary about forced disappearances in Mexico. One evening, she leaves her office after a late work meeting, intending to go home and send the documentary to her collaborators and relatives, as well as victims and specialists interviewed for the film. Upon arriving home though, she discovers that her apartment has been raided – worst of all, she realizes that the laptop containing the finished documentary footage is missing (with no backup available). What would you advise in this situation?

Sample response Tool to Use (from the Toolkit): Immediate Response Measures

Recommendations:

- Notifying her contacts of what has just happened, especially those involved in the production of the film;
- Changing all passwords for her online accounts, and enabling 2-step verification where there is the option of doing so;
- Establishing a security protocol for handling and distributing edited footage in the future;
- Asking her if she has any physical or cloud backups of any raw footage, recorded interviews, images etc. that she can recover and store securely;
- Reviewing any files that can be recovered to take stock of she has available, in addition locating any of the devices or equipment she used to record and edit the documentary;

CASE 2

> Olga is an activist – soon, she will begin working with a group of other women activists to document feminicides in Mexico. They will need to share documents online and discuss sensitive information over the phone, and some of the women will be commissioned to travel to certain cities for interviews with families. What do you recommend?

Sample response **Tool to Use (from the Toolkit):** Security Protocols

Recommendations:

- Have a group meeting to make a risk assessment
- Agree on the digital security measures that the group will have to implement as well as the travel protocol
- Agree on using a safe app to exchange messages such as Signal
- Explore safe ways to exchange documents, maybe encrypting them with GPG or sending them through a safe email account such as Tutanota o Riseup.

CASE 3

> Nelly is the coordinator of a project dedicated to the delivery of justice for women in her country. She was invited to give a presentation abroad, being in the airport discovers that she has remained her plan without data and has decided not to buy more balance or minutes since she will leave her country. While waiting for the plane she wants to check her mail by connecting to the airport's wi-fi network, what should she do?

Sample response **Tool to Use (from the Toolkit):** VPN

CASE 4

> Ariadna is an Ecuadorian journalist who is working on the investigation of a case of diversion of funds. To this end, she is making a requests for information to its government. What would you advise her to use to make the request securely?

Sample response Tool to Use (from the Toolkit): Tor Browser & Anonymous Email Account

CASE 5

> A feminist collective that defends women's right to decide has been harassed for a week on social networks, what could they do to protect themselves?

Sample response Tool to Use (from the Toolkit): Gender-Based Risk Model

Recommendations:

- The collective can analyze the risks of the attacks, the impacts and probabilities that the risk can increase or the violence escalate, and in this way define the tools and strategies to deal with.

Part 2 – Ready, Set, Go!

4. Divide the participants into teams depending on the size of the group – so that everyone can participate and contribute equally, it is not recommended for group sizes to exceed 5 participants. Remember to let each team choose a fun, creative name for themselves!
5. Now that the teams finalized and the stations are set up, explain the rules of DigiSec Rally to participants:

- According to the routes and station order established in the **Station Order and Team Route Guide**, indicate to each team at which station they should begin and at which station they will end – be sure to point out where each station is to participants ahead of time so they don't get lost!
- Teams must solve a case at each station, using what they've learned from the training and the **Case Toolkit** you've given them – they can be creative in their responses: just like in the real world, there is no "one size fits all" solution to any of the cases!
- Give teams a moment or so to prepare themselves – then call out **"Ready, Set, Go!"**
- The first team to work through each of the cases at every station and make it back to the starting point is the winner!

6. Once both teams have completed the entire rally course, hold a closing circle. In the circle, each team should explain their responses for each case, explaining the process by which they determined each of their solutions. Provide active feedback to teams as they explain their recommendations for each case.

Part XVIII

Appendix

IWPR's Digital Security and Capacity Tool (DISC)

- **Objective(s):** To gauge participants' existing digital security skill level, while also providing qualitative information on strengths and areas for improvement at a more granular, practice-specific level. disc tool is also a useful way to track their learning and comprehension progress.
- **Format:** Appendix
- **Needed materials:**
  - Copies of the DISC questionnaire

Internal document with Scores

To Be Completed at Baseline and every six months, or at end of Training Period, as appropriate.

Below you will find a series of questions that will allow your trainer to both understand the level of digital security practices within your organization, as well as to monitor any progress that it made thanks to the training you will or have received. The results are purely for monitoring and evaluation purposes and will only be shared anonymously within IWPR

and with the donors supporting this project.

Country .....

At your organization:

1. The operating system and software I use to work have been updated: (please circle)

- Never (0 points)
- In the last 6 months (1 point)
- Within last 30 days (4 points)
- Within last 15 days (5 points)
- More than 6 months ago (0 points)
- We have the newest system installed on this computer (5 points)
- They are being updated at this moment (3 points)
- I don't know that information (0 points)

2. ¿Do you backup your data through an external hard-drive or a cloud service: (please circle)

- Never (0 points)
- More than a year ago (0 points)
- In the last year (1 point)
- In the last 6 months (2 points)
- Within last 60 days (3 points)
- Within last 30 days (4 points)
- The data has been backed up within the last 14 days (5 points)
- I don't know that information (0 points)

3. Are your hard drive or cloud service encrypted?

- Yes, both are encrypted (5 points)
- No (0 points)
- Only one of them is encrypted (3 points)
- I don't know that information (0 points)
- If you answered affirmatively, which encryption tool do you use?

  .....

4. The computer I use for work has original licensed software (for example Microsoft Windows, Microsoft Office, Adobe Photoshop, Adobe Illustrator, Corel Draw, Antivirus) or open source software programs (Open office, Scribus).

- Every program is pirated (0 points)
- Some programs are pirated (1 point)
- Most programs are licensed originals (2 points)
- All programs are licensed and original (5 points)
- Most programs are open source (2 points)
- All programs are open source (5 points)
- I am not sure (0 points)

5. Anti-virus programs are loaded on the computer and the mobile phone that I use to work, are up to date and run each time the equipment is turned on.

- Yes, computer and mobile phone (5 points)
- Only on my computer (3 points)
- Only on my mobile phone (3 points)
- I don't have anti-virus programs (0 points)
- I don't know if I have an antivirus program on all my devices (0 points)
- If affirmative, which antivirus do you have on your computer?

  .....
- If affirmative, which antivirus do you have on your phone?

  .....

6. I have locked my office computer screen/cellphone with a password for the screen lock.

- Yes (5 points)
- No (0 points)
- Only one of those devices has a password (2 points)

7. The Wi-Fi network where I work has a different password from the one that the internet service provider gave me, and it meets the standards

for a strong password (Criteria: 1. includes at least 25 characters and, 2. includes both letters and numbers, and 3. Includes special characters, and 4. includes both lowercase and capital letters).

- Yes - password changed and meets at least two of the criteria for strong passwords (5 points)
- No - servicer provider password was maintained (0 points)
- Partially - only one of the criteria for passwords mentioned above has been applied (3 points)
- Partially- the password was changed but none of the criteria for passwords were applied (1 point)

8. About the use of public Wi-Fi in hotels, airports or cafés

- I never use public Wi-Fi in hotels, airports or cafés unless I connect through a virtual private network (VPN) service. (5 points)
- I sometimes use public Wi-Fi in hotels, airports or cafés without connecting through a VPN service. (2 points)
- I always use public Wi-Fi in hotels, airports or cafés without a VPN service. (0 points)

9. About the back up of my work documents, I use file encryption tools for saving documents in my laptop

- Yes (5 points)
- No (0 points)
- Only for some documents (3 points)
- If you answered yes, which file encryption tool do you use?

  .....

10. Regarding the text via email or SMS between the members of your organization.

- I always use encryption for email, SMS or chats to transmit sensitive data (5 points)
- I usually use encryption for email, SMS or chats to transmit sensitive data (3 points)
- I rarely use encryption for email, SMS or chats to transmit sensitive data (2 points)

- I never use encryption for email, SMS or chats to transmit sensitive data (0 points)

11. I share my passwords with (please circle all that apply):

- Intimate partner (0 points)
- Siblings and/or parents (0 points)
- Best friend (0 points)
- Work colleagues (0 points)
- No one (5 points)

12. Secure passwords have at least 25 characters (letters, numbers, special characters, small and capital). Do not use words from the dictionary, birthdays or any personal information. All my passwords meet these standards identified above to ensure a strong password.

- Yes (5 points)
- No (0 points)
- Only some of them (3 points)

13. I have different passwords for each of my devices and accounts (computer, phone, email, social media, bank etc)

- Yes (5 points)
- No (0 points)
- I have a few different passwords that I use, but sometimes repeat (1 point)
- Some of my passwords are set by default by my organization/office/provider of service (3 points)

14. I have made a strategic decision about how to manage my social media identities for my private, work/activism accounts based on my level of risk.

(For example using false/different identities and accounts for activism/work, or openly using my real name, photo and identity if I don't feel under threat …)

- Yes - I have considered it and feel secure with my current management of online identities (5 points)
- No - I haven't thought about it (0 points)

- Partially- I consider it may make sense to create different or more anonymous online identities but haven't made the changes yet (2 points)
- Partially - I have considered my online identities and made the changes, but I am still not sure if the setup is secure (4 points)
- My situation means that it makes more sense for me to use my own name and real identity in all my social media accounts (5 points)

15. I store my passwords in a password protected secure digital key-chain

- Yes (5 points)
- No (0 points)
- Only some accounts (3 points)
- I don't know what that is (0 points)
- Where is the key chain stored and in what format?

16. When you are browsing do you always navigate with HTTPS?

- Yes (5 points)
- No (0 points)
- What is that? (0 points)
- I always check it but it is not always possible to navigate with HTTPS (3 points)

17. About your personal social media accounts.

- All my posts on social media are public (0 points)
- I don't know who can see my posts on social media (0 points)
- I choose specific settings for each post (4 points)
- I adjust the settings to control who can see which information on my social media accounts (5 points)
- I don't know how to set admin controls on any of my social media accounts (0 points)

18. click on links or open attachments in emails when: (please circle the dates closest to clicking)

- They seem to contain important or urgent information (0 points)

- I know the sender, but unexpected email (ex. Emotional Partners, old friends) (1 point)
- They come from my trusted network (2 point)
- I expected them (3 points)
- I know and verified the sender (5 points)

19. I use secure chats and secure online voice communications tools (VOIP) for my communications.

- Yes (5 points)
- No (0 points)
- Sometimes (2 points)
- I don't know what this is (0 points)
- Which secure tools do you use?

  .....

20. I use power regulators to protect my important electronic devices from electrical surges:

- Yes (5 points)
- No (0 points)
- Only at my office (2 points)
- Only at home (2 points)
- Only for some devices (2 points)

Add up the points and record them on the Organizational Scorecard. ..... points/ 100 points

Example training agendas

- **Format:** Appendix

Although we are aware that the final content of a training session will be based on the diagnosis each trainer does of the group the will work with and we invite each trainer to adjust this session to better meeting the needs of the group, we do suggest a few options for what we think could be regular scenarios of trainings.

The example agendas below are organized by length (in days), and then by participant skill level. Other planning parameters will of course inform the ultimate design of your training; however, time is almost always the most critical:

How much time you have available ultimately determines how much content you can cover in a single workshop; this is furthermore determined by the collective skill level of the participants.

You're more likely to know how many hours or days are available to work with a group before knowing other factors, such as the venue, the number of participants, or their collective skill level.

Example Agendas for 1-Day to 1.5-Day Workshops

1.5-Day Introductory Workshop on Risk Assessment

Approximate Time Required: 10 hours

This training agenda was planned for a scenario involving a 1.5 day introductory digital security workshop, with a group of WHRDs or a women's collective, oriented primarily around general risk assessment. Ideally, the outcome of this workshop is that women participants can more easily identify their perceived risks, and can more clearly articulate their digital security needs.

This agenda includes sessions on basic digital security, self-care practices and techniques for documenting and responding to abuse or threats. For this scenario, a follow-up strategy would need to be crafted by the trainer to address the results of participants' risk assessment(s).

1. Exercise: The rules of the game[1] (Trust-building exercises[2])
2. Exercise: Defenders bingo[3] (Trust-building exercises[4])
3. Session: Personal perceptions of security[5] (Rethinking our relationship with technology[6])
4. Exercise: Who do you trust?[7] (Trust-building exercises[8])
5. Session: Your rights, your technology[9] (Rethinking our relationship with technology[10])
6. Exercise: Gender-based risk model[11] (Determining the best solu-

[1] https://cyber-women.com/en/trust-building-exercises/the-rules-of-the-game/

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

[3] https://cyber-women.com/en/trust-building-exercises/defenders-bingo/

[4] https://cyber-women.com/en/trust-building-exercises/

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

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

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

[8] https://cyber-women.com/en/trust-building-exercises/

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

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

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

tion[12])

7. Exercise: Building feminist self-care[13] (Self-care[14])
8. Session: Building stronger passwords[15] (Digital security basics 1[16])
9. Session: How to secure your computer[17] (Digital security basics 1[18])
10. Session: Safe browsing[19] (Digital security basics 1[20])
11. Session: Privacy[21] (Privacy[22])
12. Session: Mobile phones 1[23] (Safer mobiles[24])
13. Session: Let's start a documentation journal![25] (Online violence against women[26])
14. Exercise: Feminist flowers[27] (Closing and review exercises[28])

1-Day Awareness Training for WHRDs Dealing with Online Harassment

Approximate Time Required: 5 hours

This training agenda was planned for a scenario involving a 1 day introductory digital security workshop with WHRDs who have just begun to deal with incidents of online harassment. Ideally, the outcome of this workshop is that women participants can more clearly articulate their digital security needs, and can more quickly identify warning signs or patterns of online gender-based violence.

[12] https://cyber-women.com/en/determining-the-best-solution/
[13] https://cyber-women.com/en/self-care/building-feminist-self-care/
[14] https://cyber-women.com/en/self-care/
[15] https://cyber-women.com/en/digital-security-basics-1/building-stronger-passwords/
[16] https://cyber-women.com/en/digital-security-basics-1/
[17] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/
[18] https://cyber-women.com/en/digital-security-basics-1/
[19] https://cyber-women.com/en/digital-security-basics-1/safe-browsing/
[20] https://cyber-women.com/en/digital-security-basics-1/
[21] https://cyber-women.com/en/privacy/privacy/
[22] https://cyber-women.com/en/privacy/privacy/
[23] https://cyber-women.com/en/safer-mobiles/mobile-phones-1/
[24] https://cyber-women.com/en/safer-mobiles/
[25] https://cyber-women.com/en/online-violence-against-women/lets-start-a-documentation-journal/
[26] https://cyber-women.com/en/online-violence-against-women/
[27] https://cyber-women.com/en/closing-and-review-exercises/feminist-flowers/
[28] https://cyber-women.com/en/closing-and-review-exercises/

This agenda includes sessions about defining safety and security on a personal level, basic digital security practices and recognizing patterns of abuse and harassment.

1. Exercise: The rules of the game[29] (Trust-building exercises[30])
2. Exercise: Tricky candy[31] (Trust-building exercises[32])
3. Session: Personal perceptions of security[33] (Rethinking our relationship with technology[34])
4. Session: Building stronger passwords[35] (Digital security basics 1[36])
5. Exercise: Symbolic violence[37] (Online violence against women[38])
6. Exercise: Time to watch![39] (Sexting[40])
7. Session: Sexting[41] (Sexting[42])
8. Exercise: Our Reflection[43] (Self-care[44])

1-Day Risk Assessment Training for WHRDs Dealing with Online Harassment

Approximate Time Required: 7 hours

This training agenda was planned for a scenario involving a 1 day workshop with WHRDs who are dealing with ongoing incidents of online harassment, and who need support developing security plans and response strategies. Ideally, the outcome of this workshop is that women participants can more clearly articulate their digital security needs, feel more in

[29] https://cyber-women.com/en/trust-building-exercises/the-rules-of-the-game/
[30] https://cyber-women.com/en/trust-building-exercises/
[31] https://cyber-women.com/en/trust-building-exercises/tricky-candy/
[32] https://cyber-women.com/en/trust-building-exercises/
[33] https://cyber-women.com/en/rethinking-our-relationship-with-technology/personal-perceptions-of-security/
[34] https://cyber-women.com/en/rethinking-our-relationship-with-technology/
[35] https://cyber-women.com/en/digital-security-basics-1/building-stronger-passwords/
[36] https://cyber-women.com/en/digital-security-basics-1/
[37] https://cyber-women.com/en/online-violence-against-women/symbolic-violence/
[38] https://cyber-women.com/en/online-violence-against-women/
[39] https://cyber-women.com/en/sexting/time-to-watch/
[40] https://cyber-women.com/en/sexting/sexting/
[41] https://cyber-women.com/en/sexting/sexting/
[42] https://cyber-women.com/en/sexting/sexting/
[43] https://cyber-women.com/en/self-care/our-reflection/
[44] https://cyber-women.com/en/self-care/

control of their personal risk environment, and are able to develop a responsive, context-specific security plan and protocol for themselves.

This agenda includes sessions about defining safety and security on a personal level, basic digital security practices and gender-based risk assessment.

1. Exercise: The rules of the game[45] (Trust-building exercises[46])
2. Session: Personal perceptions of security[47] (Rethinking our relationship with technology[48])
3. Exercise: Who do you trust?[49] (Trust-building exercises[50])
4. Exercise: Gender-based risk model[51] (Determining the best solution[52])
5. Session: Privacy[53] (Privacy[54])
6. Exercise: Doxxing the Troll[55] (Online violence against women[56])
7. Exercise: Building feminist self-care[57] (Self-care[58])

Example Agendas for 3-Day Workshops

3-Day Introductory-Level Training

Approximate Time Required: 15 hours

[45] https://cyber-women.com/en/trust-building-exercises/the-rules-of-the-game/
[46] https://cyber-women.com/en/trust-building-exercises/
[47] https://cyber-women.com/en/rethinking-our-relationship-with-technology/personal-perceptions-of-security/
[48] https://cyber-women.com/en/rethinking-our-relationship-with-technology/
[49] https://cyber-women.com/en/trust-building-exercises/who-do-you-trust/
[50] https://cyber-women.com/en/trust-building-exercises/
[51] https://cyber-women.com/en/determining-the-best-solution/gender-based-risk-model/
[52] https://cyber-women.com/en/determining-the-best-solution/
[53] https://cyber-women.com/en/privacy/privacy/
[54] https://cyber-women.com/en/privacy/privacy/
[55] https://cyber-women.com/en/online-violence-against-women/doxxing-the-troll/
[56] https://cyber-women.com/en/online-violence-against-women/
[57] https://cyber-women.com/en/self-care/building-feminist-self-care/
[58] https://cyber-women.com/en/self-care/

This training agenda is designed for a 3-day long workshop with beginner-level WHRDs who have not yet had a great deal of (or any) prior exposure to digital security practices. Introducing basic digital security and risk assessment practices, with an explicit parallel emphasis on self-care strategies, this training agenda would be appropriate for either an organizationally-focused workshop or a workshop for a mixed group of WHRDs from different collectives or countries within the same region.

Furthermore, this agenda will prepare the group for an intermediate level follow-up training (see 3-Day Intermediate-Level Training example below); however, it can also be used for a standalone workshop.

1. Exercise: The rules of the game[59] (Trust-building exercises[60])
2. Exercise: Defenders bingo[61] (Trust-building exercises[62])
3. Session: Personal perceptions of security[63] (Rethinking our relationship with technology[64])
4. Exercise: Who do you trust?[65] (Trust-building exercises[66])
5. Session: Your rights, your technology[67] (Rethinking our relationship with technology[68])
6. Session: How does the internet work?[69] (Digital security basics 1[70])
7. Exercise: Feminist flowers[71] (Closing and review exercises[72])
8. Exercise: Gender-based risk model[73] (Determining the best solution[74])

[59] https://cyber-women.com/en/trust-building-exercises/the-rules-of-the-game/
[60] https://cyber-women.com/en/trust-building-exercises/
[61] https://cyber-women.com/en/trust-building-exercises/defenders-bingo/
[62] https://cyber-women.com/en/trust-building-exercises/
[63] https://cyber-women.com/en/rethinking-our-relationship-with-technology/personal-perceptions-of-security/
[64] https://cyber-women.com/en/rethinking-our-relationship-with-technology/
[65] https://cyber-women.com/en/trust-building-exercises/who-do-you-trust/
[66] https://cyber-women.com/en/trust-building-exercises/
[67] https://cyber-women.com/en/rethinking-our-relationship-with-technology/your-rights-your-technology/
[68] https://cyber-women.com/en/rethinking-our-relationship-with-technology/
[69] https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/
[70] https://cyber-women.com/en/digital-security-basics-1/
[71] https://cyber-women.com/en/closing-and-review-exercises/feminist-flowers/
[72] https://cyber-women.com/en/closing-and-review-exercises/
[73] https://cyber-women.com/en/determining-the-best-solution/gender-based-risk-model/
[74] https://cyber-women.com/en/determining-the-best-solution/

9. Exercise: The act of NO[75] (Self-Care[76])
10. Session: Building stronger passwords[77] (Digital security basics 1[78])
11. Session: Safe browsing[79] (Digital security basics 1[80])
12. Session: Malware and viruses[81] (Digital security basics 1[82])
13. Exercise: Building feminist self-care[83] (Self-care[84])
14. Session: How to secure your computer[85] (Digital security basics 1[86])
15. Session: What does your metadata say about you?[87] (Safe online advocacy[88])
16. Exercise: Marco Polo[89] (Safer Mobiles[90])
17. Session: Mobile phones 1[91] (Safer Mobiles[92])
18. Session: Networked publics[93] (Privacy[94])
19. Session: Privacy[95] (Privacy[96])
20. Session: Let's start a documentation journal![97] (Online violence against women[98])

[75] https://cyber-women.com/en/self-care/the-act-of-no/
[76] https://cyber-women.com/en/self-care/
[77] https://cyber-women.com/en/digital-security-basics-1/building-stronger-passwords/
[78] https://cyber-women.com/en/digital-security-basics-1/
[79] https://cyber-women.com/en/digital-security-basics-1/safe-browsing/
[80] https://cyber-women.com/en/digital-security-basics-1/
[81] https://cyber-women.com/en/digital-security-basics-1/malware-and-viruses/
[82] https://cyber-women.com/en/digital-security-basics-1/
[83] https://cyber-women.com/en/self-care/building-feminist-self-care/
[84] https://cyber-women.com/en/self-care/
[85] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/
[86] https://cyber-women.com/en/digital-security-basics-1/
[87] https://cyber-women.com/en/safe-online-advocacy/what-does-your-metadata-say-about-you/
[88] https://cyber-women.com/en/safe-online-advocacy/
[89] https://cyber-women.com/en/safer-mobiles/marco-polo/
[90] https://cyber-women.com/en/safer-mobiles/
[91] https://cyber-women.com/en/safer-mobiles/mobile-phones-1/
[92] https://cyber-women.com/en/safer-mobiles/
[93] https://cyber-women.com/en/privacy/networked-publics/
[94] https://cyber-women.com/en/privacy/privacy/
[95] https://cyber-women.com/en/privacy/privacy/
[96] https://cyber-women.com/en/privacy/privacy/
[97] https://cyber-women.com/en/online-violence-against-women/lets-start-a-documentation-journal/
[98] https://cyber-women.com/en/online-violence-against-women/

3-Day Intermediate-Level Training

Approximate Time Required: 15 hours

This training agenda is designed for a 3-day long workshop with WHRDs who have already had a more introductory level training (see 3-Day Intermediate-Level Training example above) and is intended to be offered as a follow-up. It is considerably more technical in nature than the introductory-level agenda, focusing on practical applications of digital security concepts as well as critical thinking skills for informed decision making on tool use. It also goes more into depth on topics such as women and technology, privacy, encryption and anonymity.

If working with participants from the same organization, this training will also provide them with strategic approaches to begin sharing their knowledge with others at their organization, including designing organization security plans and protocols.

1. Exercise: Tricky candy[99] (Trust-building exercises[100])
2. Exercise: I decide[101] (Determining the best solution[102])
3. Session: Her-story of technology[103] (Rethinking our relationship with technology[104])
4. Exercise: Ask me anything![105] (Privacy[106])
5. Session: Apps and online platforms: friend or foe?[107] (Privacy[108])
6. Session: Safe online campaigning[109] (Safe online advocacy[110])
7. Session: Mobile phones 2[111] (Digital security basics 1[112])

[99] https://cyber-women.com/en/trust-building-exercises/tricky-candy/
[100] https://cyber-women.com/en/trust-building-exercises/
[101] https://cyber-women.com/en/determining-the-best-solution/i-decide/
[102] https://cyber-women.com/en/determining-the-best-solution/
[103] https://cyber-women.com/en/rethinking-our-relationship-with-technology/herstory-of-technology/
[104] https://cyber-women.com/en/rethinking-our-relationship-with-technology/
[105] https://cyber-women.com/en/privacy/ask-me-anything/
[106] https://cyber-women.com/en/privacy/privacy/
[107] https://cyber-women.com/en/privacy/apps-and-online-platforms-friend-or-foe/
[108] https://cyber-women.com/en/privacy/privacy/
[109] https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/
[110] https://cyber-women.com/en/safe-online-advocacy/
[111] https://cyber-women.com/en/safer-mobiles/mobile-phones-2/
[112] https://cyber-women.com/en/digital-security-basics-1/

8. Session: Introduction to encryption[113] (Encryption[114])
9. Session: Encrypted communication[115] (Encryption[116])
10. Exercise: The cauldron[117] (Closing and review exercises[118])
11. Session: Storage and encryption[119] (Digital security basics 2[120])
12. Exercise: Secret friend[121] (Anonymity[122])
13. Session: Anonymity[123] (Anonymity[124])
14. Session: Digital security decisions[125] (Determining the best solution[126])
15. Session: Organizational security plans and protocols[127] (Planning ahead[128])
16. Exercise: Love Letter to Myself[129] (Self-care[130])

3-Day Advanced-Level Training

Approximate Time Required: 12 hours

This training agenda is designed for a 3-day long workshop with WHRDs who have already progressed through introductory and intermediate-level trainings (see prior examples) and are ready for more advanced-level experience.

[113] https://cyber-women.com/en/encryption/introduction-to-encryption/
[114] https://cyber-women.com/en/encryption/
[115] https://cyber-women.com/en/encryption/encrypted-communication/
[116] https://cyber-women.com/en/encryption/
[117] https://cyber-women.com/en/closing-and-review-exercises/the-cauldron/
[118] https://cyber-women.com/en/closing-and-review-exercises/
[119] https://cyber-women.com/en/digital-security-basics-2/storage-and-encryption/
[120] https://cyber-women.com/en/digital-security-basics-2/
[121] https://cyber-women.com/en/anonymity/secret-friend/
[122] https://cyber-women.com/en/anonymity/anonymity/
[123] https://cyber-women.com/en/anonymity/anonymity/
[124] https://cyber-women.com/en/anonymity/anonymity/
[125] https://cyber-women.com/en/determining-the-best-solution/digital-security-decisions/
[126] https://cyber-women.com/en/determining-the-best-solution/
[127] https://cyber-women.com/en/planning-ahead/organizational-security-plans-and-protocols/
[128] https://cyber-women.com/en/planning-ahead/
[129] https://cyber-women.com/en/self-care/love-letter-to-myself/
[130] https://cyber-women.com/en/self-care/

This workshop – more tactical in nature than the previous trainings - focuses less on leveraging conceptual knowledge into development of practices for specific tools, and more on real world scenario-based applications of critical thinking and decision making skills (which also allows you, as the trainer, to more comprehensively assess the overall progress of the group).

1. Exercise: [Charades!] (Closing and review exercises[131])
2. Session: Safer websites[132] (Safe online advocacy[133])
3. Exercise: More online identities![134] (Anonymity[135])
4. Session: Let's reset![136] (Digital security basics 2[137]
5. Exercise: Doxxing the troll[138] (Online violence against women[139])
6. Session: Digital security plans and protocols: post-training replication[140] (Planning ahead[141])
7. Exercise: The loving touch[142] (Self-care[143])
8. Exercise: DigiSec rally[144] (Closing and review exercises[145])

[131] https://cyber-women.com/en/closing-and-review-exercises/
[132] https://cyber-women.com/en/safe-online-advocacy/safer-websites/
[133] https://cyber-women.com/en/safe-online-advocacy/
[134] https://cyber-women.com/en/anonymity/more-online-identities/
[135] https://cyber-women.com/en/anonymity/anonymity/
[136] https://cyber-women.com/en/digital-security-basics-2/lets-reset/
[137] https://cyber-women.com/en/digital-security-basics-2/
[138] https://cyber-women.com/en/online-violence-against-women/doxxing-the-troll/
[139] https://cyber-women.com/en/online-violence-against-women/
[140] https://cyber-women.com/en/planning-ahead/digital-security-plans-and-protocols-post-training-replication/
[141] https://cyber-women.com/en/planning-ahead/
[142] https://cyber-women.com/en/self-care/the-loving-touch/
[143] https://cyber-women.com/en/self-care/
[144] https://cyber-women.com/en/closing-and-review-exercises/digisec-rally/
[145] https://cyber-women.com/en/closing-and-review-exercises/