Training Toolkit

FEMINIST CYBERSECURITY

Prepared by: **Nadine Moawad**
Translated by: **Farah Kobeisy**
Reviewed by: **Hayat Mirshad**

FE-MALE
LOUD- PROUD- FEMINISTS

ABOUT FE-MALE

Fe-Male is a civil feminist collective working with women and girls to eliminate injustice through building young feminist movement, empowering agents of change, and campaigning together against discriminatory norms and policies.

Beirut, Sami El Solh
Near Lebanese University Faculty of Fine Arts, Furn El Chebbak Public Garden Street, Al Hayek Building, Ground Floor

009611380873

info@fe-male.org

www.fe-male.org

FeMaleComms

- **The Feminist Cybersecurity Training Toolkit is produced by Fe-Male**
- **in partnership with The International Center for Non-profit Law (ICNL).**

This report is wholly financed by the Government of Denmark.
The Government of Denmark does not necessarily share the opinions here within expressed.
The author bears the sole responsibility for the content.

MINISTRY OF FOREIGN AFFAIRS OF DENMARK
Danida

HOW TO USE THIS TOOLKIT

We developed **this toolkit** to help feminists in our region plan and run digital security workshops in their communities and organizations. Of course, plenty of terrific feminists have developed several digital security manuals over the years and we've linked to plenty of great content you can discover under different sections. This one, in particular, was based on the results of a Feminsit Cybersecurity Survey we ran in April 2021 with regional WHRDs, in addition to three training workshops we ran in Beirut and online for the regional audience.

There are differing views on how to build digital resilience for our activist communities. More and more trainers are moving away from the "workshop" formula. The model for this was you send someone from the organization to attend a few days of digital security training and expect that they implement what they learned for their organization. This was followed by a "training of trainers" model that hoped to broaden knowledge and have more hands available to help with amplifying security practices.

In 2015, **Tactical Tech** published very useful research that evaluated 10 years of digital security training you can check it out here

https://secresearch.tacticaltech.org/

Since 2015, more trainers have moved to an "accompaniment" model where a security expert accompanies an organization for a year or more to build capacity and also help implement policies. Several also recommend budgeting and hiring full-time technologists in large organizations to hold this work. The end goal is similar across these attempts: protect human rights defenders and organizations from digital vulnerabilities, surveillance, hacks, and censorship.

Feminists have traditionally added two important elements to this digital security movement. One is that gendered lack of confidence with technology is a crucial area we need to counter in our movements. Two is that one cannot possibly work with technology as merely a tool without engaging with the political environment that governs tech spaces and policies.

In this spirit,

we recommend that you use this toolkit for two purposes:

1

To help you develop your feminist lens on internet politics and economics - in addition to security. Digital security work in our movement has often kept us on the defensive. We need to take more proactive approaches to securing ourselves, as well as contributing our analysis to the policy and design of the internet.

2

To understand the overarching principles of digital security because recommended tools and apps change every day. The math, however, stays the same. We've designed this manual to help you gain confidence and learn strategy so that, in the future, you can decide which tool suits you for what purpose and for how long.

This toolkit serves as an introductory booklet to a topic that is both changing daily and extremely broad. It's 2021 and we face compounding global and local problems. Any number of issues can lay claim to extreme priority importance. And yes, technology governance is one such issue. We encourage you to delve into your own areas of interest and hope that these pages will excite you - and boost your confidence - about the possibilities of feminist engagement with tech.

PLANNING YOUR AGENDA

You will need to adjust your agenda depending on how much time you have allocated. It is possible to squeeze your agenda to achieve at least one learning outcome per hour. And it is possible to use several more hours for the same learning outcome. Of course, more time allows for deeper learning. But often, this is out of our control and depends on the host organization's time and budget.

In general terms, we recommend:

- **Always** including a political discussion element to your talk or training, no matter how short your time is. Never separate digital security from the socio-economic policy context.
- **Always** prioritize security principles over security tools - because tools change.
- **Always** use exercises that start from a personal connection to technology. This helps demystify the idea that only engineers understand tech.

Methodology Pointers:

When training from a feminist lens, it's good to keep the following in mind:

- Be careful not to speak as the expert who holds all the knowledge. Your goal is not to inspire expertise, but to encourage confidence in researching and validating information readily available on the open internet.
- Don't be hesitant to say "I don't know, I will look it up" if you are not sure about an answer.
- Avoid describing tech aspects as "too complicated" or out of one's league.
- If you are working with feminist groups, tap into their own expertise and knowledge in analyzing the policy environment of the internet.

Learning Outcomes & Measuring Impact

Learning outcomes are important for any teacher or trainer. What is your goal from each session? What will participants gain by the end of it? If you go into your session with a clear objective in mind, you can stay focused on achieving it.

Think of phrasing your learning outcomes in the following structures:

By the end of this session,

participants will be able to identify

By the end of this session,

participants will understand

By the end of this session,

participants will download and run

You can measure the **impact of your training** by using an evaluation form or by using a pre/post test that you administer before the training starts and then after the training is completed. This test can measure an increase in knowledge, a change in attitude, or a gaining of skill

Here are some examples:

Testing for Knowledge

If you are giving a session on internet governance, you can test the increase in knowledge with an example like this:

Who decides internet policies?

- Governments
- Technical communities
- Corporations
- Civil society
- All of the above (correct answer)

If you are training on security principles, you can test the increase in knowledge with an example like this:

State two overarching principles of digital security

Testing for Attitudes

Attitudes measure a personal reflection and are a great method for measuring if you have managed to increase confidence with tech. You can check how they answered before the workshop and how (hopefully) they increased the score post-workshop. Here are some examples:

I understand how digital risks work (rank from 5-1)

- I feel it is possible to be highly secure online (rank from 5-1)
- I feel that I can make solid decisions about which secure tools to use (rank from 5-1)

AGENDA TEMPLATE

When planning your agenda, remember that preparation and more preparation is key - especially when you are just starting out in this field. The more details you include in your agenda, the better prepared you are for the session.

Time frame	Session Title	Learning Outcome	Session Breakdown & Notes	Facilitator(s)	Material Needed

Here's an example of an agenda for a -4hour training focused on safe browsing:

Time frame	Session Title	Learning Outcome	Session Breakdown & Notes	Facilitator(s)	Material Needed
30 minutes	Setting the Space	By the end of this session, participants will get to know each other and learn about the shared expectations of this workshop space. They will also set and learn what the rules of the space are.	The facilitator welcomes all participants to the training and asks everyone to introduce themselves and share expectations from the workshop (15 minutes) Participants collectively set the rules of the "safe space" (15 minutes)	Maha (lead facilitator) Samia (support)	Large post-it notes of 5 colors Flip chart paper Markers Pens
60 minutes	How Browsers Work	By the end of this session, participants will be able to explain how browsers work technically and identify the areas of risk associated with .browsing	The expert gives a presentation on the technicalities of web browsers and explains where the security risks lie (45 minutes) Participants ask clarification questions (15 minutes)	Sara (expert) Maha (support)	Projector HDMI cable Laptop Slide deck
Coffee Break					
90 minutes	Hands-On Exercise: Securing Browser	By the end of this session, participants will switch to a secure browser and install add-ons and clean up their old browsing info from laptops and mobiles	The expert gives a presentation on recommended tools for 30) secure browsing (minutes Participants are guided by the facilitator to work on their laptops and mobiles to switch to safer browsing with 60) support of expert (minutes	Sara (expert) Maha (support)	Projector HDMI cable Laptop Slide deck USB drives with software installation packs
30 minutes	Closing and Evaluation	By the end of the session, participants will evaluate and solidify their learning	The facilitator sums up the learnings of the day and asks participants to share an evaluation of what they have learned and what support they would like for the future.	Maha (lead (facilitator	Printed evaluation forms

*** TIP:** Make a hard copy of your agenda to keep with you during the training and make any notes on it of how things went in the actual sessions. Perhaps you had to add more time to an outcome or an exercise didn't go as well as planned. That way you can go back to your hard copy when preparing for your next training and remember what worked and what needs improvement.

*** REMINDER:** Allocate enough lost time for any hands-on application of secure software with participants. Many hiccups may arise: no battery, installation not working, slow internet connection, participants familiarizing themselves with the software.

Ice Breaking Exercises

Sharing Experiences

2 minutes per participant

When going around the room to have participants introduce themselves, use a prompt that connects them to technology. One pleasant example encourages participants to think back on their earlier experiences with the internet. **Here are some examples:**

- **Tell us about your first ever experience with the internet**
- **What is the first thing you ever looked up online?**
- **Tell us about your first blog or digital content post**

You can also think of prompts that open up participants' imagination around technology. **Here are some examples:**

- **If you have unlimited funding, what new technology would you create?**
- **If you had a robot assistant, what functions would you program them to do daily?**
- **What's an idea for an app you always thought would be useful?**

* **REMINDER:** The goal of the exercise is to open up discussion and get participants comfortable with the space, not necessarily a teaching moment. It is recommended that the statements you choose are topics you will come back to during the training, so that participants feel they have learned more about these issues.

Spectrum Exercise

30 - 15 minutes

Ask participants to line up on a spectrum from strongly agree to strongly disagree, with the option to find a middle if they are unsure. Share statements about internet rights and see where the participants move. Take a few comments from different sides of the room. Encourage participants to move if they have heard a convincing argument or changed their mind. **Here are some examples of statements:**

- **There is no privacy on the internet anymore so we shouldn't bother**
- **I'd advise my teenage niece not to send nudes**
- **Social media companies offer more freedom of expression than traditional media**
- **It is possible to be very secure in online communications**
- **Anonymity encourages online violence**
- **Governments should block porn websites because they are harmful**

SECTION 1:

A FEMINIST LENS ON TECHNOLOGY

We are all familiar with gender discrimination in technology - although programming started originally as a “women’s job”. Girls are less likely to be encouraged to study science or math - we know this. Tech domains suffer from “bro culture” and sexism towards women - we also know this well. It is a fact that we need to remove the barriers keeping girls discouraged from science and technology to better reflect the shared experiences and interests of women in these fields. But this is not where we stop. We need a feminist approach to technology design and policy - particularly today in 2021 when tech developments are exponentially moving us towards a new form of surveillance capitalism.

Debunking the Myth It is easy for techies to make women feel like technology is not their domain. You might feel at a disadvantage because you didn’t study computer science or engineering.

But think for a minute about other domains.

- X You do not need to be a mechanical engineer to know that bus routes connect communities and foster economic participation.
- X You do not need to be an electrician to know that access to affordable electricity is a human right.
- X You do not need to be a chemist or a pharmacist to know that everyone needs to have easy access to life-saving medication.

Technology is a manifestation of human creativity, of problem-solving and we can all participate in it - and we should open up the spaces that allow us to do so.

The best place to start for exploring feminist takes on technology is the Feminist Principles of the Internet, developed and maintained by APC and a large network of feminist tech groups from around the world. Visit www.feministinternet.net to browse through the 17 principles - each discussing a feminist standpoint on technology issues. Let's go through a few of them here.

Depending on the time available, and the interest of the group, you may choose to open a discussion into one or more debates around tech. The Feminist Internet website has plenty of great introductory exercises to get participants to think - themselves - about what a feminist internet does or looks like or facilitates. We've adapted one exercise suggestion here:

Exercise: Imagine a Feminist Internet

30-20 minutes

Material needed: sticky notes, markers, flip charts

In groups or individually, ask participants to think of what a feminist internet means to them. You can use prompts like: "In a feminist internet…." or "A feminist internet is…" which they can complete with a word or a phrase or a paragraph. They may write the ideas on colorful post-its or on flipchart paper or on a shared doc online. It is time for them to explore and dream. It may be necessary to "warm up" the idea by asking for some basic ideas of what a feminist internet would look like.

The facilitator collates these ideas, pulls out the key words, and groups them by connectedness. The discussion can deepen with participants defining what they found most important overall or simply provide an entry point to open a presentation.

Another way to do this exercise is to ask participants to "vote" on their most-liked keywords by sticking little dots on the cards to show their support for an idea. They must have a limited number of "dots" they can give and can be allowed to stick all of them on a single idea to show weight. This is useful once the facilitator has grouped or summarized the inputs.

ACCESS TO THE INTERNET

FACILITATOR NOTES

One methodology you can use for a discussion session is the following:

1. Start with a prompt question and ask participants to have a quick chat with their neighbor about the topic (5 minutes). **Examples are:**

- **Should access to the internet be considered a human right?**
- **Why is there a gender gap in access to the internet?**
- **How much do you pay for your internet access? How does this bill compare to other monthly bills?**
- **How does internet speed affect your usage?**

2. Ask participants to share some reflections with the rest of the group (-5 10 minutes)

3. Give a short presentation on some of the current debates on access to the internet. A good place to start is with explaining the history of internet cable infrastructure and showing some maps. Most participants will be surprised to learn that the internet passes through large cables laid out across oceans and territories. Find a map of your country's oceanic and land cables. Reflect on how decisions are made on where to place the maps, who pays for them, when maintenance or upgrades are scheduled, etc.

4. Present the Feminist Principle on Access and allow time for questions and comments.

PRESENTATION CONTENT

Feminist Principle on Access

A feminist internet starts with enabling more women and queer persons to enjoy universal, acceptable, affordable, unconditional, open, meaningful and equal access to the internet.

Public vs. Private Access

Establishing access to the internet as a human right was first proposed at the United Nations by the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression in 2011. However, debates around the standards of internet access continue among the technical community, private sector, governments, and civil society, with varying and often competing interests in connecting the remaining %40 of the global population to the internet. Private corporations claim to be connecting more folks to the internet via their "free" access programs like Facebook's Free Basics app or Google Balloons. What they provide via these programs, however, is access only to their corporate apps or services. This is a terribly restricting feature - from the world's richest companies - that is more about user creation and data collection than actual access to the free and open internet. It places great limitations on new users' understanding and imagination of the network. The feminist principle on access emphasizes the kind of internet we want: affordable, equal, and universal, and is especially significant when we look at the current digital gender gap affecting internet users today.

The Gender Gap in Internet Access

Amidst these debates, women in developing countries are often instrumentalized as a vulnerable target group rather than a stakeholder group with a crucial say the kind of internet access that guarantees rights rather than restricts them. The Web Foundation estimates that "men remain %21 more likely to be online than women, rising to %52 in the world's least developed countries." There are several underlying reasons for the gender gap — including affordability, education and digital skills, income levels, or living in rural areas.

Region	Women's Internet Use	Men's Internet Use	Gender Usage Gap
North America	94%	95%	1%
Latin America	60%	64%	12%
Europe	77%	81%	5%
Middle-East and North Africa	77%	79%	9%
Sub-Saharan Africa	28%	38%	43%
Central Asia	57%	64%	15%
East Asia	83%	86%	2%
South East Asia-Pacific	60%	67%	11%
South Asia	18%	37%	137%

Source: **www.webfoundation.org (March 2020)**

INTERNET GOVERNANCE

FACILITATOR NOTES

When training on internet rights, participants will want to know how exactly they can influence these. It is not intuitive to most people that internet policy is decided by humans. Most think this is in the realm of tech engineers only. So it's important that you encourage participants to bring a feminist lens to policy advocacy efforts on technology. **Here are some ideas for prompts to begin the discussion:**

1. Ask the group if they have ever read the Community Guidelines or Terms and Conditions of a social media network like Instagram or Twitter. If you have an extra 10 minutes, ask them to look up and read these guidelines on the spot.

2. Take a few minutes to ask participants to explain to the rest of the group the guidelines. What surprised them? Was it easy to understand? What are flagrant rules they weren't fully aware of?

3. Move to explaining how different entities (corporations, governments, technical communities) decide on their policies and protocols. A history of internet protocols would also be useful. Your goal is to help participants understand that humans (mostly white cis-men) make daily decisions and rules about the internet. And that they can choose to be part of these discussions from a feminist perspective.

4. Present the Feminist Principle on Governance and allow time for questions and comments.

Presentation Content

Feminist Principle on Governance

We believe in challenging the patriarchal spaces and processes that control internet governance, as well as putting more feminists and queers at the decision-making tables. We want to democratize policy making affecting the internet as well as diffuse ownership of and power in global and local networks.

How Can I Influence Tech Policy?

The United Nations created the Internet Governance Forum (IGF) **www.intgovforum.org** in 2006 to facilitate a global discussion of public policy issues pertaining to the internet. The IGF is a multi-stakeholder platform, which means that it brings together governments, technical communities, the private sector, and civil society at the same table.

Building towards the global IGF, which is held every year, are national country-level forums and regional forums (like the Arab IGF).

The IGF itself does not issue binding language or resolutions, meaning that it does not dictate policy. However, it is a great space to:

1. Discuss emerging issues related to internet governance

All panels and workshops at the IGFs are determined by an open and consultative process. So any organization may propose putting a discussion and speakers on the agenda. Because it is a "multi-stakeholder" forum, the organizing body tries to ensure that different groups are talking to each other - as opposed to civil society only discussing matters by itself.

2. Debate governments and corporations around internet rights

Telecom Ministers and other government officials often attend regional and global IGFs. Depending on the region, some IGFs are government-heavy (like the Arab IGF) and others have stronger activist organizing behind them. Tech giants like Facebook, Google, and Microsoft also usually send their policy delegations to IGFs. It is, therefore, useful for civil society and internet freedom activists to attend these forums and organize events to meet, lobby, or debate government and private sector representatives.

3. Lobby UN officials for internet policy

Although the IGF itself cannot issue binding high-level documents, i.e. UN countries do not vote, language from IGF statements or reports can make it into other UN spaces. Special rapporteurs, for example, do sometimes attend IGF events to learn about tech-related issues. If your goal is to influence UN language on freedom of expression or violence against women - as it pertains to the internet - you can check for UN agencies attending the IGF and make your advocacy plans.

4. Advance a feminist agenda

Women and queer representation at the IGFs has grown over the years, but it is still a struggle, especially at the Arab IGFs. Feminists have lobbied for different processes and initiatives at the IGF, for example, taking stock of women speakers on panels and gender issues on the agenda. A good place to connect with this work, if you are planning to attend an IGF is here:

https://www.intgovforum.org/multilingual/content/gender-and-internet-governance

For sexual rights activists, APC has developed a curriculum on Sexuality & Internet Governance. The modules can help you understand internet governance and issues of intersectionality and sexuality-related content online. It is available online here:

https://en.ftx.apc.org/shelves/sexuality-and-internet-governance

Civil Society Internet Forums

While the IGF is a formal, multi-stakeholder convening, civil society has created several annual meetings to advance the discussions on internet freedoms. Here are some forums you can look up and check for opportunities to attend or participate remotely.

Bread & Net - a MENA-focused internet rights convening

https://www.breadandnet.org/

- RightsCon
- MozFest
- Internet Freedom Festival
- MisInfoCon
- RightsCon
- Internet Freedom Festival
- SXSW
- Global Privacy Summit
- re:publica
- Stockholm Internet Forum
- Privacy Risk Summit
- Allied Media Conference
- DEF CON
- Global Voices Summit

The Complete Feminist Principles of the Internet

A feminist internet works towards empowering more women and queer persons in all our diversities to fully enjoy our rights, engage in pleasure and play, and dismantle patriarchy. This integrates our different realities, contexts and specificities including age, disabilities, sexualities, gender identities and expressions, socioeconomic locations, political and religious beliefs, ethnic origins, and racial markers. The following key principles are critical towards realizing a feminist internet.

ACCESS

1. Access to the internet

A feminist internet starts with enabling more women and queer persons to enjoy universal, acceptable, affordable, unconditional, open, meaningful and equal access to the internet.

2. Access to information

We support and protect unrestricted access to information relevant to women and queer persons, particularly information on sexual and reproductive health and rights, pleasure, safe abortion, access to justice, and LGBTIQ issues. This includes diversity in languages, abilities, interests and contexts.

3. Usage of technology

Women and queer persons have the right to code, design, adapt and critically and sustainably use ICTs and reclaim technology as a platform for creativity and expression, as well as to challenge the cultures of sexism and discrimination in all spaces.

MOVEMENTS & PUBLIC PARTICIPATION

4. Resistance

The internet is a space where social norms are negotiated, performed and imposed, often in an extension of other spaces shaped by patriarchy and heteronormativity. Our struggle for a feminist internet is one that forms part of a continuum of our resistance in other spaces, public, private and in-between.

5. Movement building

The internet is a transformative political space. It facilitates new forms of citizenship that enable individuals to claim, construct and express selves, genders and sexualities. This includes connecting across territories, demanding accountability and transparency, and creating opportunities for sustained feminist movement building.

6. Internet governance

We believe in challenging the patriarchal spaces and processes that control internet governance, as well as putting more feminists and queers at the decision-making tables. We want to democratize policymaking affecting the internet as well as diffuse ownership of and power in global and local networks.

ECONOMY

7. Alternative economies

We are committed to interrogating the capitalist logic that drives technology towards further privatization, profit and corporate control. We work to create alternative forms of economic power that are grounded in principles of cooperation, solidarity, commons, environmental sustainability, and openness.

8. Free and open source

We are committed to creating and experimenting with technology, including digital safety and security, and using free/libre and open source software (FLOSS), tools, and platforms. Promoting, disseminating, and sharing knowledge about the use of FLOSS is central to our praxis.

EXPRESSION

9. Amplifying feminist discourse

We claim the power of the internet to amplify women's narratives and lived realities. There is a need to resist the state, the religious right and other extremist forces who monopolize discourses of morality, while silencing feminist voices and persecuting women's human rights defenders.

10. Freedom of expression

We defend the right to sexual expression as a freedom of expression issue of no less importance than political or religious expression. We strongly object to the efforts of state and non-state actors to control, surveil, regulate and restrict feminist and queer expression on the

www.feministinternet.netinternet through technology, legislation or violence. We recognize this as part of the larger political project of moral policing, censorship, and hierarchisation of citizenship and rights.

11. Pornography and "harmful content"

We recognise that the issue of pornography online has to do with agency, consent, power and labour. We reject simple causal linkages made between consumption of pornographic content and violence against women. We also reject the use of the umbrella term "harmful content" to label expression on female and transgender sexuality. We support reclaiming and creating alternative erotic content that resists the mainstream patriarchal gaze and locates women and queer persons' desires at the center.

AGENCY

12. Consent

We call on the need to build an ethics and politics of consent into the culture, design, policies and terms of service of internet platforms. Women's agency lies in their ability to make informed decisions on what aspects of their public or private lives to share online.

13. Privacy and data

We support the right to privacy and to full control over personal data and information online at all levels. We reject practices by states and private companies to use data for profit and to manipulate behavior online. Surveillance is the historical tool of patriarchy, used to control and restrict women's bodies, speech and activism. We pay equal attention to surveillance practices by individuals, the private sector, the state and non-state actors.

14. Memory

We have the right to exercise and retain control over our personal history and memory on the internet. This includes being able to access all our personal data and information online, and to be able to exercise control over this data, including knowing who has access to it and under what conditions, and the ability to delete it forever.

15. Anonymity

We defend the right to be anonymous and reject all claims to restrict anonymity online. Anonymity enables our freedom of expression online, particularly when it comes to breaking taboos of sexuality and heteronormativity, experimenting with gender identity, and enabling safety for women and queer persons affected by discrimination.

16. Children and youth

We call for the inclusion of the voices and experiences of young people in the decisions made about safety and security online and promote their safety, privacy, and access to information. We recognize children's right to healthy emotional and sexual development, which includes the right to privacy and access to positive information about sex, gender and sexuality at critical times in their lives.

17. Online violence

We call on all internet stakeholders, including internet users, policy makers and the private sector, to address the issue of online harassment and technology-related violence. The attacks, threats, intimidation and policing experienced by women and queers are real, harmful and alarming, and are part of the broader issue of gender-based violence. It is our collective responsibility to address and end this.

SECTION 2:
ORGANIZATIONAL CYBERSECURITY

The cybersecurity of an organization - or group or collective or network - requires **two main elements:**

1

Policy - this is the set of rules you decide on for how to protect yourselves and how to respond to threats

2

Practice - this is the daily routine everyone needs to participate in to ensure the policy is actually put into action

DEVELOPING YOUR POLICY

A great tool to get you started is Ford Foundation's Cybersecurity Assessment Tool **(CAT)**

https://www.fordfoundation.org/work/our-grants/building-institutions-and-networks/cybersecurity-assessment-tool/

It is a questionnaire that will take you about 15 minutes to fill and will cover four different areas of cybersecurity: operational, devices, accounts, and associated risks. Don't worry about having a lot of "I don't know" or "No" answers. The tool should not overwhelm you. Rather, it should give you a holistic view of all the areas of cybersecurity policy that you need to develop. Once completed, you will get several pages of recommended next steps for each section.

It is very useful to seek the help of a cybersecurity expert to accompany you in setting the policy and switching your practices. Several organizations and activists offer free support and we've included a list of these here. If you are a smaller activist collective, you can still work through the different elements of your policy and practice using the tools recommended here and do some extra research and testing of solutions.

For larger institutions, ideally, if you are able to raise funds and allocate resources for this, you must aim to include cybersecurity costs in your core operational budget line. Think of it similarly to how you think of legal fees or how you used to think of IT support. Your longer-term plan must be to have a tech consultant on retainer or an in-house technologist to support you, the same way you'd have a lawyer on retainer or on staff.

Most feminist groups like to think of holistic approaches to security rather than isolate cybersecurity as a separate matter. This is good practice as it allows you to connect several aspects of security together because they are often linked.

Examples of Sections of a Cybersecurity Policy

Data

What kind of data does your organization store? How do you store it safely? Who has permissions to access it? For what purpose? When is it deleted? Do you use a cloud service (for example Google Drive)? Or do you use a local storage (for example a server in your office)? How do you do regular back-ups and what are the risks of losing the data?

Passwords

What are the rules for individual passwords on your network? How often should the team change their passwords? Where are they allowed to store them? How long should a password be? Who has access or permission to reset people's passwords? Should we log out daily?

Communications

Which platforms must be used for communications (email, mobile, video calls, etc)? Which platforms should we not use at all for our group or organization? Who has access or permissions to see content of communications? Who can see the logs?

Machines

Do you offer laptops or mobile phones for work only? What permissions does a staff member have to download software or content on these machines? Can we take them with us when we travel? How do we protect them from viruses?

Incident Response

What do we do if someone loses their mobile phone? Or when a social media account is hacked? Or if we are attacked online? How do we act if we discover malware that has been copying our files? Or if there is an accident in the office and we lose our server?

Website

How do we maintain the security of our website? What about financial security if we accept donations on the website? How can people communicate with us securely?

SOAP Policy-Building Tool

https://usesoap.app/

SOAP is a free, online security policy generator. It asks you questions and, as you answer them, you are building your security policy. This gives you a great start - much better than a blank page. The acronym stands for Securing Organizations with Automated Policymaking. And along the way, SOAP provides support and implementation tips to ensure the entire process is as easy as possible.

DEVELOPING YOUR PRACTICE

Rules, of course, mean nothing if they are not adopted and enforced by the group collectively. Always remember that the internet is a network of computers and that any group using the internet is a network of users. We must use the power of the network to our advantage, but this also means that one vulnerable user on our network puts us all at risk.

For example, if your organization is using Google Workspace for all its email communication and file storage, every google account needs to be strongly protected (a strong password, two-factor authentication, etc). It is enough for one member of the team to not take their security seriously for our adversaries to get into our network and have access to all the files and emails. People find many excuses to drop secure practices. For example, someone might be too lazy to log out or to use a long password. Or you might just postpone resetting your password for weeks or even months, reusing the same password that you have shared with your roommates for the wifi.

Good practice requires a supportive culture. If all of us are using secure apps, for example, we encourage each other to use them. Think of putting in regular check-ins for secure practice, as well as finding the most user-friendly secure tools for your team to enjoy.

Security is similar to a cat-and-mouse game. The cat is always trying new tactics to catch the mouse and the mouse is always developing strategies to escape the cat. It is not enough to have one workshop or implement one tool to think that we are secure. It is a constant discussion that must happen in our movements. Our task is never to be %100 secure - otherwise we would not leave our homes nor do activism at all. Our task is to make it more expensive and more time-consuming for our opponents to hack us. The worst we can do is get lazy or complacent with security so that all our opponents have to do is take a peek over our shoulders. Remember that the math is on our side: one small step (an extra password, for example) forces our opponents to use much larger steps (a more expensive supercomputer to hack us).

THREAT MODELING

The first step in planning your cybersecurity - whether as an individual or as a group - is to **understand the risks** you are up against. What are the sources of risk? What are the consequences of breaches? What indicates that you have to switch to an emergency plan or to activate a security protocol? Without a plan in place, you cannot respond wisely to situations. It is also important to note two points:

1

You must **revise your plans** on a consistent basis. This could be every quarter or every year. Remember that we are in a live battle with our opponents. They are developing their plans and so must we.

2

You must **test your plans** during quiet moments. When a team is prepared for an emergency protocol, they are more likely to deal with it calmly and practice their response. Don't wait for a security breach to happen to test your plan. Create a fake emergency and test your team's preparedness. Oftentimes, this is the best way to learn, adjust plans, and allocate proper resources.

Among the good examples of threat modeling exercises is this one from the Electronic Frontier Foundation (EFF). More here: **https://ssd.eff.org/en/module/your-security-plan.** You can start your threat modeling by answering these five important questions:

What do I want to protect?

Who do I want to protect it from?

How bad are the consequences if I fail?

How likely is it that I will need to protect it?

How much trouble am I willing to go through to try to prevent potential consequences?

Let us examine each question.

What do I want to protect?

Make a list of all of your technology-related assets. These could be software or hardware, files and emails or mobile phones and cameras. One likely important asset is a database of sorts. If you work with survivors of violence, for example, and store their information in an excel sheet, this is a very valuable asset. Your contact list. Your emails. Your social media accounts. Laptops and chargers, mobile phones and chargers, etc. Photo albums - perhaps you collect evidence of human rights violations and have photographic evidence. Perhaps you have scanned copies of testimonies or reports that you want to use in a court case.

All of these are examples of assets you must identify. Make a table of these: what are they, where are they stored, who has access to them and why? Once you have identified your assets and organized this information, you can take a wider look and start to plan how you will protect them.

* **REMINDER:** Keep your asset list up to date! Set a monthly or quarterly reminder to update any new data or equipment.

Who do I want to protect it from?

Now, looking at each of your assets, start to identify who you want to protect it from. Who is the source of risk who might want to hack your devices or look at your accounts? If you are documenting state violations, for example, authorities might be trying to access your files. If a certain source is trying to discredit you, they might be wanting to "plant" damaging information on your devices. A thief might be trying to snoop into your finances to figure out how to steal from you. Your boss might be trying to read your emails. Your ex-partner might be trying to read your mobile messages. A troll army might be trying to steal your twitter account.

Understanding the source of the threat helps us demystify our opponents and their capabilities to put the better plans in place to secure our assets.

* **REMINDER:** Remember that, as feminists, we understand that gender-based violence often happens in our most intimate circles. So we know that sources of threat could always include intimate partners, family members, neighbors, etc.

How bad are the consequences if I fail?

This question is closely linked to the final question: what am I willing to do? It is important for your group to identify the consequences of breached security. Is someone's safety directly linked to the protection of their data? For example, if you organize with queer folks in extremely hateful contexts, a bad security plan might pose a direct threat to someone's life. If you are planning a protest in an authoritarian context, security forces who breach your communications might arrest and jail the organizers.

For other, less crucial data, the consequences might be restricted to embarrassment or minor financial loss. These are still important to identify.

* **REMINDER:** Often, for feminists, our personal lives and lifestyles are used as ammunition to discredit us. So even if you have separate devices for work, your personal devices still need protection. Adversaries might leak personal photos or chat logs to smear or "expose" you. So make sure you think about this additional gendered dimension when doing your threat modeling.

How likely is it that I will need to protect it?

It is important to distinguish between what might happen and the probability of it happening. Calculating risks is all about estimating probability - based on your knowledge and experience. The moment we step out of the door in the morning, we start to face risks. But we don't address this by staying indoors. We take measured steps to mitigate and minimize the risk.

Of course, the probability of risk changes depending on a lot of factors. If your group is currently operating under the radar, then perhaps it is unlikely that your adversaries know of your activities. If, on the other hand, your group is partaking in a public media conversation about a "controversial" issue (for example, a particular case of gender-based violence has caused public uproar) and you are in the spotlight, then it is more likely that your opponents will try to attack you.

* **REMINDER:** Don't forget the particular risks of your context - these might be so banal that you forget to include them. If you live in a city with daily power cuts, for example, you need to allocate for outage-related risks.

* **Tip:** Develop your own red-orange-yellow system for collective agreement on the likelihood of attacks during particular times. Put a protocol in place to raise the preparedness level of your team during more difficult times.

How much trouble am I willing to go through to try to prevent potential consequences?

This is the final question you need to answer with utmost honesty. Often, when we attend a digital security workshop, we get so excited about using complex tools. But back at our office desks, we get bored or lazy and end up using nothing. It is more important to commit to minimum effort you know you can do than to plan for maximum effort that you won't end up doing.

As mentioned earlier, this question is closely linked to the consequences of security breaches. If you perceive the consequences as super urgent, you will want to add a few minutes to your daily login / logout practices. Or you may want to add a few thousand dollars to your organization's security budget to buy better machines or stronger locks. You must decide together what balance of time, cost, and convenience you are willing to take to ensure your network's security.

* **REMINDER:** Every one step you take towards security is a thousand steps your hacker needs to add to their attack plan. The difference between an -8character password and a -24character password is literally a matter of seconds for you but it means more resources and time for your hacker.

Overarching Principles of Cybersecurity

As mentioned earlier, this question is closely linked to the consequences of security breaches. If you perceive the consequences as super urgent, you will want to add a few minutes to your daily login / logout practices. Or you may want to add a few thousand dollars to your organization's security budget to buy better machines or stronger locks. You must decide together what balance of time, cost, and convenience you are willing to take to ensure your network's security.

One: Choose Open-Source Software

All software is written using a programming language that tells the code what to do and how to interact with the user. Our interactions with the software follow the same logic: we put in some kind of input (for example, we ask the laptop calculator 1+1=?) the software processes this request (checks for the answer in its coded database) and provides an output (usually the answer on the screen "2").

How can we know if a software or program on our laptops is only doing the processing it is showing us and not, for example, secretly activating our microphones to record us?

The only way to know for sure what the software is doing is to see the source code, i.e. the original "recipe" of the program. If the source code is locked, we call this closed-source or, as is often the case: proprietary software. This means that it's copyrighted and/or locked. We are not allowed to see it. Therefore, we cannot change it or copy parts of it. We cannot verify %100 that it is

doing what it says it is doing. We have to trust the programmer or the corporation. This puts us at a significant disadvantage and risk.

With open-source software, however, the code is shared publicly and transparently. Often, other programmers are allowed to modify the code as they'd like to build new code like add-ons or mods. Seeing the code allows us to trust it. Therefore, open-source software are recommended alternatives to closed or proprietary software.

Since the early days of programming, folks who believe in freedom and openness of code - for the public good and also for security and trust - have organized within the FOSS (Free and Open-Source Software) movement. It is sometimes referred to as FLOSS to emphasize that Free means freedom (Libre) not free of charge.

Anti-capitalist feminists will recognize the potential of FOSS as a liberation project, especially as software becomes more and more a means of organizing labor and even of production of value. Do not worry about reading the coding language yourself. There are hundreds of thousands of FOSS activists and hackers around the world who are always checking the code and keeping us up-to-date. Just because you are not an engineer and cannot build a bridge yourself, it doesn't mean you cannot form an opinion about the design and policy of bridges to benefit society and the public good.

Proprietary Software	Open Source Alternatives
Microsoft Office (Word, Excel, etc.)	LibreOffice
Internet Explorer (browser)	Firefox (a much better browser)
WhatsApp	Signal
Windows (operating system)	Linux
Zoom (video conferencing)	Jitsi

Two: Encrypt Everything

You have used encryption your whole life - mostly in the form of passwords. But even as a child in school, when you passed a piece of paper to your classmate, you probably wrote it in code so that the teacher cannot understand it even if they intercepted the message. This is the basic tenant of encryption: you and I agree on a secret key to understand each other without others understanding what we are talking about.

Sometimes, it is easy for someone to guess the key. It might take them a few seconds or a few hours. They can guess it by trial and error or by a smarter strategy. We all played these brain games as kids, trying to decipher a secret message. Now replace the human brain (and its processing limitations) with a super computer that can process a billion times faster. It can attempt to guess if your password is any word in the dictionary in only a few minutes. It can attempt every book title ever recorded, every song title, every famous name or location on earth, in only a few hours. Your job now is to be smarter than this supercomputer.

Needless to say, you need a smart password strategy to keep your accounts and devices secure. Having a group / organizational / network password policy helps standardize. It is also important to understand the underlying principles of passwords so you know why you should use two-factor authentication, for example, not just that you should use it.

Passphrases not Passwords

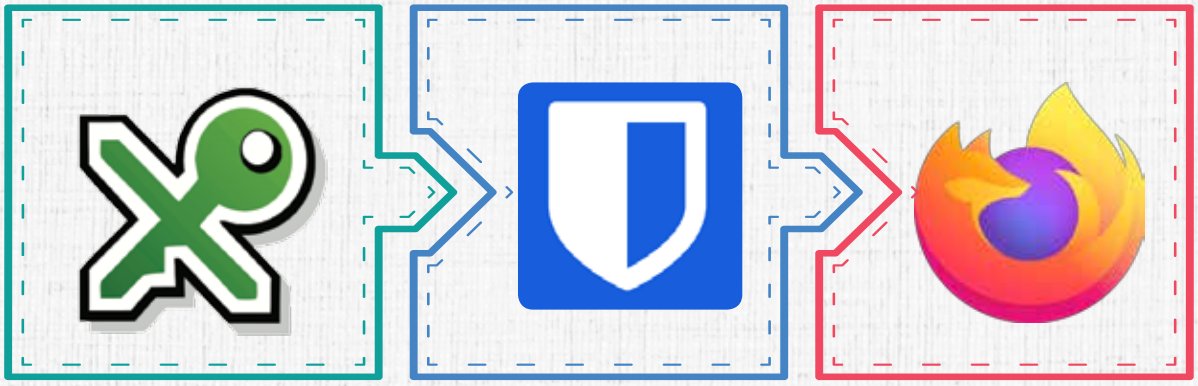
"Passphrase" is a smart way to remember that the length of your password is the most important feature. You must never sacrifice the length. Most services force you to use special characters such as %$#! in addition to numbers (3 ,2 ,1…) and capital letters, but will allow only 8 characters. This is not smart practice. Aim for passwords of 16 characters or longer. Aim for entire phrases. Since we are Arabic speakers, it is useful to use Arabic phrases since they are not available in the English-language dictionary.

This XKCD comic on passwords generated quite the discussion. The math is correct, but folks argued that supercomputers will just attempt to run different combinations of dictionary words and can eventually crack these passwords. Of course, this is true, although it takes much longer times than shorter passwords. The point of the comic is spot-on when combining difficulty to remember with difficulty to guess. This is why your threat modeling asks: how much trouble are you willing to go to to protect your data?

Password Managers

Using a password manager can be very useful if you'd like to have super passphrases on your accounts. This solves the problem of remembering too many long passwords because, remember, you should never use the same password on multiple accounts. If one of your accounts is compromised, then all of your accounts are at high risk.

A password manager solves this problem by asking you to remember only one super long password. This allows you to open a "vault" that has all your super long passwords for accounts stored. Then you can copy and paste them into your browser.



/https://www.keepassx.org

/https://bitwarden.com

https://www.mozilla.org/en-US/firefox

KeePassX

KeePassX is a popular password manager that can also be run from an external drive like a USB.

BitWardn

BitWarden is a new program for password management that is gaining popularity.

FireFox

FireFox have added a "Master Password" or Primary Password to their in-browser settings. You can use this to store passwords in FireFox more securely.

Practicing Secure Online Communications

PROTECTING YOURSELF FROM VIRUSES

Your device security depends primarily on the software functioning as you want it to function. This is why we worry about viruses. Regardless of other security measures you take, if there is **malicious software (malware)** on your device, it threatens everything. All devices are at risk of malware, though at varying degrees. Laptops running Windows are especially vulnerable.

A great resource for detailed protection against malware is available from Tactical Tech's Security-in-a-Box and you can access it on this

URL https://securityinabox.org/en/ /guide/malware

Generally, as a trainer, you must stay updated on recent malware practices and new tricks. Security experts recommend the following for how to with malware:

1. Educating users on know how malware works and staying vigilant

2. Supporting users to use anti-virus programs and keep security tools up-to-date

3. Teaching users how to eliminate threats when they find them

4. Encouraging users to switch to safer, less risky tools where possible.

UNDERSTANDING MALWARE

Malware is the general term that includes viruses, spyware, worms, and trojans. You can explain it as a code that infiltrates (secretly) your device in order to do something malicious. Sometimes this is part of a large scam like stealing your credit card information or your passwords. Sometimes it has less serious motives to scare users or demonstrate hacker skills. Governments can use targeted malware, for example, to spy on citizens. Thieves can spread malware, for example to get you to wire money under false pretenses. And computer companies can also spread malware, for example to get you to make certain purchases.

Malware spreads over the internet through emails or downloads. One common way is called phishing, where a hacker tries to trick you into installing malware yourself using social engineering.

Avoiding malware

With good secure practices, you can take preventative steps to protect yourself from malware. Here are some recommended tips:

- Keep your operating system (Windows, Mac, Android, iOS) up-to-date. These companies try to keep their software secure from recent known malware. So updating your system will take advantage of the company updates. Avoid using "cracked" operating systems or software as these make you vulnerable to malware.

- Schedule a day every few months to clean up your device. Uninstall programs you no longer use. Update programs you use often, like your browser or email client. Update your mobile apps or set it on automatic update.

- Always be very careful about installing programs from unofficial websites. This is a common way that hackers try to trick you. Check the URL you are downloading from. Avoid using third-party websites. If you have doubts, do not download the item. The same applies to email attachments and links sent to you over messages. If it looks suspicious, do not open it. The same applies to USBs or hard-drives, which are becoming less common but could also have malicious content.

• Shortened URLs can be hiding a malicious link behind them - and are difficult to judge by just looking at them. If you suspect a shortened URL, use

/https://www.checkshorturl.com

to reveal what is behind it.

Anti-virus software

You can do your best to protect yourself from malware, but you still need to keep an anti-virus software running and scan your device regularly. There is currently no single recommended anti-virus software that is open-source.

If you are using Windows, their built-in protection mechanism, Windows Defender, is a good option when kept up-to-date. Here are some other software options you can explore:

AVIRA **https://www.avira.com**

AVG **/https://www.avg.com**

AVAST **https://www.avast.com**

Malware Bytes **https://www.malwarebytes.com**

Recovering from Viruses

You can look for signs in your daily usage that your device might be infected. Has it slowed down suddenly? Are programs behaving in odd ways? Are you getting strange pop-ups? If you have a suspicion, run an antivirus scan right away. Disconnect from the internet. More often than not, the antivirus will take care of the issue. You can also restore your device to factory settings to wipe out all information from it (be careful about backing up important files first). If you need further help, call an expert or a hotline.

Safe Browsing

*** REMINDER:** This applies to your mobile phone as well! Download the Firefox mobile app for Android or iOS and use it for safer browsing on your mobile.

Browsing is a very common way to get infected with malware. Hackers will often use fake websites or phishing websites to get code into your browser or into your device. So securing your browser and developing safe practice is very important.

We recommend using Mozilla Firefox for your daily web browsing because it is a free and open source web browser with terrific add-ons to help increase privacy and security. When training on browser safety, it is a good idea to do a hands-on exercise to download Firefox and switch from all other web browsers.

Download the latest version of Firefox from the official website

https://www.mozilla.org

While you're on the Mozilla Foundation website, check out other useful tools they have developed for privacy and security.

As a trainer, it's good to stay up-to-date with new security plugins and add-ons, and here are the two most recommended as a start:

HTTPS Everywhere

(https://www.eff.org/https-everywhere)

Privacy Badger

(https://www.eff.org/privacybadger)

*** Tip:** If you suspect a phishing website, you can use this tool: **https://www.phishtank.com/**

to check if a website is trying to do anything malicious such as stealing your information or downloading a virus.

You can design a training around using **Firefox** that includes:

1. Downloading to laptop and mobile
2. Switching bookmarks from other browsers and deleting them
3. Installing the 2 recommended add-ons (and others if you have time)
4. Setting up the privacy settings
5. Setting up the default search engine

A Search Engine with Privacy

Experts recommend using DuckDuckGo as a default search engine because it does not track its users or sell their search data the way most commercial search engines (like Google or Bing) do.

DuckDuckGo

Privacy & Security Settings

Firefox settings will offer a number of steps to increase your privacy while using the browser. Remember to stay updated with any changes to new or old settings! Participants can enable features to limit tracking by websites that collect (and then sell) your data and monitor your behavior on their platforms. This option is called Do Not Track and it is helpful although companies still find ways to ignore it.

Users also have options to think about how much of their browsing history they want to record. This can also be changed in the settings, as well as choices around location tracking. It's a good idea to accompany your workshop participants through each option and ask them to make changes on the spot or think about this and come back to them later.

The same applies to making decisions about security settings. We recommend checking the boxes that enable Firefox to warn you when websites try to install add-ons, or are known to be malicious or suspicious.

Participants will also probably ask about saving logins in the browser. The safer option is, of course, not to save any logins. But you might want to make exceptions for less-used websites. In this case, we recommend using **Firefox's** built-in password manager that prompts you for a Master Password before you can see your saved logins.

This is **very important** because it only takes someone a few seconds to open your saved logins if you have left the room for just a few minutes with your laptop open.

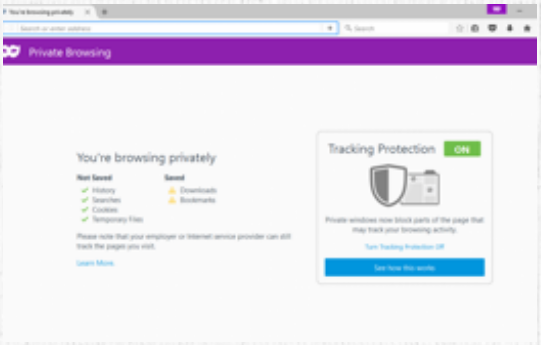
Private browsing mode

Private browsing is a good way to prevent Firefox (or any other browser) from storing data about your current browsing session, such as the URL you have visited. It does NOT, however, protect you from the website itself tracking your behavior. For more advanced anonymity online, see the next page for the **TOR Browser.**

Firefox add-ons

A Firefox add-on is software that adds new features in the form of plugins and extensions.

Here are two recommendations to use in your trainings:



HTTPS Everywhere

HTTPS Everywhere is an add-on that helps Firefox connect securely to websites that support encryption. It makes sure you are always using the HTTPS connection instead of HTTP (which is less safe). If you don't have an S at the end, it means that your connection with the website is not encrypted and that the information you are sending and receiving from the website could be monitored by your ISP or by surveillance.

Privacy Badger

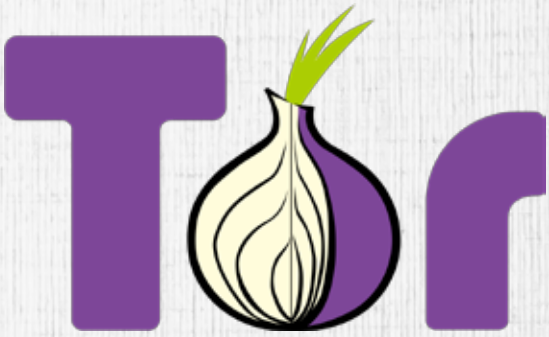
Privacy Badger is a browser add-on that prevents third-party companies from tracking your online activities. It is available for Firefox, the Tor Browser, and Chrome. Once you realize how much tracking is done from a simple web visit, you will want to turn on this option.

* **REMINDER:** Always keep your add-ons and browser up-to-date. Put in regular reminders to delete unused add-ons every few months to avoid any vulnerabilities.

Tor Browser

For advanced private browsing, you can download and use the Tor Browser, which is a project built to defend internet users from surveillance and tracking. What Tor does is relay and encrypt your connection to websites - while you are browsing - through different points in the Tor network. So trackers cannot tell what your actual information is. You will appear as a random internet user from a random location. If your government or ISP is blocking certain websites for all IPs from Egypt, for example, your Tor connection will relay you through an IP in Australia (random), so you will be able to access these websites. The Tor network is maintained by thousands of volunteer-run servers around the world.

The Tor browser is also a great way to ensure an added layer of protection for your anonymity. If you are publishing sensitive content online, you can log on to your anonymous accounts on Tor to ensure that you also have browser privacy.



Section 3: Online Violence

Technology-mediated violence against women is a recent manifestation of misogyny that feminists contend with every day. But it is also a familiar product of patriarchal norms. Women need only express an opinion online to be bombarded with gendered and sexualized attacks. This is especially accentuated when women speak of feminist issues or expose harassers or challenge authority. One can draw strong parallels between online / offline spheres - both public and private - in how misogyny is perpetuated.

Feminists for centuries have questioned the urban design of public spaces that makes for unsafe streets and squares. They have done the same for private spheres like homes and schools and workplaces, asking always: who controls the design and who sets the rules of a space so that it facilitates and - often - normalizes violence against women? The same is true of the internet. Whether highly visible on the public network or completely anonymous in a private group chat, feminists experience daily the tribulations of an internet that originally promised to set us all free of gendered bodies.

Facilitating a Workshop on Online Violence

Things to Remember

Online violence targeted at women or minorities is real and terrifying.

Up until the early 2010s, a lot of folks would argue that because it is “virtual” violence, it isn’t as alarming as “real-life” violence. Thankfully, this idea has been debunked over and over again at the expense of women who’ve had to endure horrific smear campaigns and threats on public or private platforms. When facilitating a workshop on the topic, it is important to keep this in mind.

Online violence against women can have traumatizing consequences

Some people will argue that online violence is so common, it shouldn't be so devastating. They claim it is normal for women to receive derogatory messages or unwanted sexual content. However, just because it is prevalent, doesn't mean it is not traumatizing or triggering. When preparing for a workshop on the topic, treat it the same way you would treat any discussion of violence: with care and mindfulness that it is a triggering topic for women who've experienced it - regardless of the form and extent.

Avoid victim-blaming or ideas to restrict women's expression

Deciding what to share or say or how to appear online is up to each individual's decision. Your goal as a trainer is never to tell women how to express themselves online. Be alert to interject into a discussion that has participants blaming other women for posting certain photos or opinions. Freedom of expression is not the problem here; misogyny is the problem. Our job as facilitators is to encourage participants to understand how online violence works across different experiences and to think together about resistance and remedial strategies.

There is no one-stop solution to online violence

In fact, there are a myriad of strategies to address both cases of violence and the infrastructure that allows this violence. It is similar to how we deal with family or intimate partner violence. Sometimes the legal route is a good option. Sometimes community interventions are more helpful. Sometimes it is good to lay low for a while. Sometimes amplifying feminist content is more strategic. Often, it is a combination of short-term and long-term activism.

Consent is key

Dominant online culture can sometimes rush to make a case study out of someone's traumatic experience. Campaigners may see this as an opportunity to "mediatize" the issue or raise someone's profile into the public as a survivor of violence. It is super important to stress the importance of consent during your workshop. Survivors should never be put under pressure to go under public scrutiny. Online culture attributes a certain "heroism" to survivor narratives - but this should never be at the expense of the individual's informed decision-making or personal wellbeing.

Understanding Gender-Based Violence Online

You will be able to draw on participants' own experiences with online violence. But it's also important that you familiarize yourself, as a trainer, with the many facets of this topic. This includes:

1. Knowing the context: experiences vary by culture, geography, legal environment, or language, so it's important you are familiar with the context.

2. Staying up-to-date: experiences also change over time as feminists figure out new ways to communicate and organize online and challenge misogyny, so it's important you are up-to-date with policies and strategies.

The MENA WHRD Survey (2021)

In 2021, Fe-male conducted an online survey with WHRDs from the MENA region to better understand first-hand experiences with online violence and safety online. The full report is available on www.fe-male.org and is a good resource to grasp the topic of gender-based violence online.

The highlight of the findings of this survey is the contrast between the importance of the internet for feminist activism vs. the alarming violence experienced by these same activists online.

%91.3 of the WHRD respondents said their work would be difficult or impossible without the internet. Most of them use the internet for campaigning and raising awareness on gender issues, and the overwhelming majority (%82.6) are publicly visible work online, %52.2 of which reported being very publicly visible. A clear %97 of respondents agree that "the internet is an important public sphere for advancing the issues they work on."

This undeniably shows how important it is to have an internet that is open, free, and safe for WHRDs in the MENA. And yet, the price they pay personally and professionally for their digital activism raises serious concerns. %78.3 of them reported experiencing violence online, the most common of which was sexist, racist, or homophobic messages (%55.7). An alarming %30.4 reported receiving direct attacks or threats of violence. And %9.6 faced legal action because of their online activities.

When asked about particularly gendered experiences of online attacks, an overwhelming %97.4 of respondents reported at least one form of gender discrimination. This included %53.9 receiving sexist attacks (slutshaming or gaslighting as examples), commentary on looks or lifestyle or dress (%44.3) or threats of a sexual nature (%38.3).

Highlights

Experiences with Online Violence

More than half the respondents chose to elaborate on their experiences, many of whom received **multiple forms of violence.** One respondent cited:

> "[I have received] attacks online, sexual harassment, threats of rape, shot down my instagram twice then I couldn't log in anymore because of reports. My organization's account on Twitter was disabled because of reports, my Facebook post videos constantly deleted, my organization's account on Facebook was blocked 13 times. [They created] fake profile accounts in my name on Facebook. I reported it many times but it still was not deleted. They used my name to spread fake news about me, threats for my life, sexual blackmail, hostilities, slutshaming every day."

Many respondents also reported frustration with platform regulation when it comes to both reporting harmful content and losing access to their accounts or their organizations' accounts because of reporting campaigns. This is in addition to dealing with hacking as a form of retaliation against feminist or political content.

> "The organization›s Instagram account was hacked for a full day, and we have confidential data for people who directly contact us and didn›t want any of the content to be exposed or manipulated."

It was also noteworthy that a large number of respondents discussed **prolonged online attacks that continued for months or years,** not single instances, escalating at various occasions. Most of these were related to content posted by the WHRD around feminist issues.

> "Over more than a year, I received direct death threats and intimidation, that were extended to kidnapping from a powerful political party, followed by a lawsuit against me at the military court and threats of prison."

> "I receive constant private messages of nudity and sexual content and harassment."

Attacking WHRDs' reputation was significantly reported as a sexist silencing tactic, including creating fake profiles or spreading false rumors.

> "The two most difficult experiences were when (1) I was cyberbullied with a fake account and threats after posting a concern as a statement on Facebook. (2) A campaign was created a few years ago also on Facebook attacking me and my family because of a published article in a daily newspaper. The online threat became a reality and I was also attacked several times while driving."

Attackers also commonly resort to patriarchal social norms to attack the personal looks or lifestyles of feminist activists, accusing them of ruining culture and agitating women.

> " I received messages that were insulting and undermining the overall work done for women, claiming we are destroying society and women don't need further rights."

These attacks also extend to WHRDs' children, one reported receiving "insulting messages attacking my personal life, my son and my career." Another reported receiving threats against her -10year-old daughter after a media interview about women's sexual rights. One woman reported:

> "They manipulated my posts and used them out of context in order to defame me. They posted open calls for my family to kill me as atonement."

> "I receive sexual harassment and threatening messages from lots of men because I challenge religious patriarchy. My ex-partner also threatened to kill me and kidnap my children because, he said, I was immoral being a feminist."

And so women who speak out against sexism and discrimination end up bearing the brunt of harmful online campaigns against them - using the very tools they are denouncing in the first place. There is no line drawn between the private lives of WHRDs and the content of their public posts online. Indeed, **a common strategy by attackers is to expose or threaten to expose personal details about feminists as a form of attack.**

“The most difficult experience of my life was being attacked on social media after a TV interview, in which I was advocating against child marriage and polygamy. I was accused of debauchery and blasphemy.”

“My Facebook account was monitored and they arrested me because of my activism on documenting human rights violations.”

“Whenever I share a post showing my support for LGBTQ community, I get shamed by men in private and public messages, called derogatory words for LGBTQ and sent pornographic content.”

“The state has been focused on persecuting women human rights defenders and getting them to sign pledges that they will stop using Twitter. It doesn’t matter if you have a private or public account or the number of followers - all feminists are under severe threat.”

While **sexuality content was cited as a major provoker of misogynistic comments,** WHRDs whose activism is centered on wider human rights issues also reported receiving sexist attacks just because they were women speaking out:

“The toughest experience was receiving hate mail and verbal violence because of my posts related to freedom of expression and belief.”

Effects of Online Violence

Attacks for feminist activism online take **a huge toll on WHRDs' wellbeing**. The smear campaigns often impact their access to jobs or social networks, as well as severe psychosocial damage. This is coupled with a feeling of **constant surveillance** which also drives women away from public internet spaces.

> "I get hurtful messages, often with sexual slurs. I try to ignore them but I spend the whole day worried about them."

> "I was summoned for security interrogations where I was threatened. I have a constant feeling of being watched."

Online Safe Spaces

When talking about violence, it is important to unpack its positive flip: safety. What does safety mean to participants? How do we define a safe space online or in-person?

APC has a module on Creating Safe Spaces online available here

https://en.ftx.apc.org/books/creating-safe-online-spaces

you can adapt one of their exercises and here is an example to help.

Exercise: Imagine a Feminist Internet

Time required: 40 minutes

Material needed: Flip chart paper, markers, large post-its

The main purpose of the exercise is for participants to express their own definitions of a safe space and look for shared understanding of a safe space. A group might use this as a first exercise in designing new online spaces together or in redesigning an existing one with shared values of safety in mind.

Individual visualization:

10 minutes Ask your participants to close their eyes and think about a specific place / time / circumstance in which they felt the safest. Encourage them to be specific in their visualization and describe the setting, people, climate, colors, feelings, etc. You can also ask participants to express this in drawing.

Small group discussion:

15 minutes In small groups of three to five people each, ask participants to share with one another what they have visualied. Give enough time for individual sharing and reflection.

Full group:

15 minutes To process, write «SAFE» in the middle of a sheet of flip chart paper and «mind map» the question: «What was it that made you feel safe?»

At the end of the exercise, you will have come up with a list of words, phrases and concepts that define «safe».

Notes for the trainer/facilitator:

- Look for commonalities in participants› responses but also interrogate differences in their responses.
- Pay attention and highlight factors that can be applied to online spaces
- Always synthesize key learnings from the activity to reinforce concepts.

Managing your Social Media Accounts

For many feminist activists, the decision to use social media networks like Facebook, Instagram, TikTok, or Twitter is difficult. On one hand, there is enormous reach. On the other hand, these corporations have problematic policies and are only focused on making profit. So feminist content online is packaged into data they can sell to advertisers.

You can integrate an Account Security component into your training to make sure that participants are making informed decisions about their social media usage - personally and professionally.

* **REMINDER:** If you work in a feminist organization, remember that your own personal pages are also vulnerable to misogynistic attacks, not just your organization's pages.

Discussion:

Deciding what to share online

Encourage participants to think about their own decisions of what they choose to share online and to whom. Here are some prompts to get the discussion going:

1. **Ask participants:** do you post the following information online? Is it necessary? How do you negotiate this sharing of data?

- birthday
- contact phone numbers
- addresses / locations
- details of family members
- sexual orientation or dating life
- education and employment history

2. Ask participants to reflect on this question: has a friend or contact ever shared information about you online that you did not consent to? Did they do this on purpose? Or did it happen indirectly?

3. Ask participants to reflect on a piece of personal information about them that is impossible to find online. Without revealing it, ask them to share with the group how they have avoided its publication.

4. Ask participants to look up their own names on Google (using Private browsing to avoid customized searches). What shows up? What bothers them about what shows up? Discuss.

Additional Training: If you have enough time in your training, ask participants to draw a map of their digital identity. What groups are they connected to? What keywords are associated with them? What can the public find out about their personal details?

Tactical Tech offers a great resource on

https://myshadow.org/

to do a "digital detox" of your data online. You can also use the "Trainer" section of their website for additional resources to integrate into your workshop.

Protecting Your Social Media Accounts

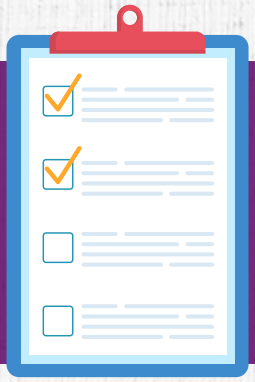
In addition to the measures previously discussed in Section 2, you can facilitate sessions focused on securing social media accounts. Most companies (including Facebook and Google) offer their own “security check-ups” that take you through various steps to securing your accounts. For some participants, this can seem rather complicated. So it is a good idea to take them through the steps in a workshop setting to build their confidence in handling these on their own.

Facebook in particular needs constant attention because it is the largest social networking site used today. Under Account Security & Privacy, participants can look at different available options and make choices about audiences and data. **It is important to remind participants that they cannot shield their data from the company itself or from its advertisers.**

So sharing info - even if private - on Facebook must be an informed decision. However, they can protect their data from being viewed from the public or from friends’ lists.

Google also offers a Privacy Checkup checklist on your account. It can alert you to weak passwords associated with your account, to browsing history, or additional back-up authentications. It is good practice to set a reminder to check this option on a regular basis.

* **REMINDER:** If you receive an email or notification that you need to secure your account, double and triple check that the URL is correct for the company sending this. The URL has to point you to facebook.com or google.com to be authentic. A security warning is a very common phishing practice. Look back at our phishing section to remind yourself how to check for suspicious links.



TWO-FACTOR AUTHENTICATION

Two-factor authentication (2FA) is important because it adds a level of security to accessing your account. It also enables you to retrieve your account if you have lost the password or it got stolen. **Make sure to ask all participants to enable this feature on all their accounts.**

Security experts actually use three factor authentications for best measure: something you know, something you are, something you have. In the case of most online companies, they provide the opportunity for you to input two of these three:

Something you know = your password

Something you have = your mobile phone that gets an SMS or push notification or code

2FA is also a good way for you to be alerted if someone is trying to hack your account. If you receive a message with an authentication co

Strategies for Responding to Violence

It is important to remember that responses to online violence are just as important in their social aspect as they are in their technical aspect. As the saying goes: there is no technical solution to a social problem.

So it is important to think with your participants about different strategies in responding to online violence. It is also important to remember and remind your participants that there is no one-size-fits all solution. The internet is a network of people and the only smart response is from a network of people - not individual routes. Here is a good exercise to think of responding to online violence:

A CALL FOR HELP

Time: 60 minutes

Material needed: Flip Chart & markers

The facilitator shares the following scenario with the group: You woke up this morning to a group email from

someone in this room addressed to everyone. In it, she says:

Friends, last night, I opened my phones to find hundreds of notifications and SMSs that are full of hateful, violent messages and threats. It is because I posted a feminist article on my profile. I don't know how it spread or who these people are or what happened. I am very scared. I don't know what to do. Please help.

Ask each participant to take 5 minutes to draft an email response. They must think about what they will say, what help they can offer, or what advice they can give. When everyone is ready, ask them to share in plenary their response.

The facilitator then takes keywords from the responses and writes them on a common flip chart. If the same keyword recurs, you can put a star next to it. When completed, you will most likely have a diversity of responses and strategies that may include:

- Using the reporting or blocking options on the platform
- Documenting the abuse with screenshots
- Offering personal and emotional support
- Legal strategies or reporting to the police
- Security strategies to secure account or temporarily disable it
- Advocacy strategies to amplify the content
- Solidarity strategies to show public support

There will also be some disagreements within the group about different strategies. **For example:**

- Should we make this a public case and highlight it in the media? Or should we keep it low profile and not spread it further?
- Should we counter the attackers with comments? Or should we not respond to trolls?
- Should we re-share the content more or should we delete the content?
- Should we call the police? Or should we address this within our own tools?

It is good to facilitate a discussion on these options: why and why not? Remember the tips shared at the beginning of this section. Consent of the survivor is always key. Sometimes multiple approaches are healthy. Sometimes they contradict each other and become useless. Some women are more comfortable with a public fight. Some women prefer not to engage.

What is important to emphasize is the power of the network in responding to these threats. Specific routes will depend on the legal or political situation in each particular context.

RESOURCES

Digital Security Helplines

Access NOW offers 7/24 digital security support, including in Arabic from their Tunis office. Visit

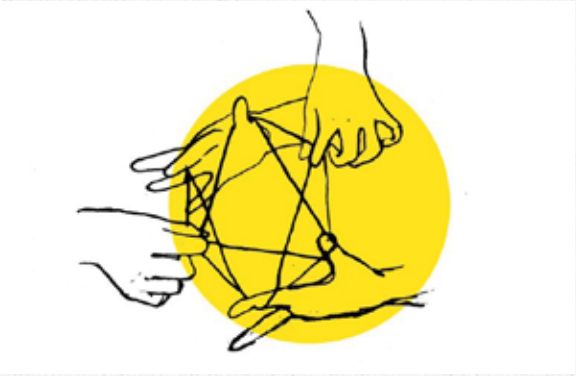
https://www.accessnow.org/help/
for more on the services or email
help@accessnow.org
for support.

SMEX offers a digital safety helpdesk for emergency support. You can message them on Signal or Whatsapp on **+961 81 633 133** or email **helpdesk@smex.org**

APC offers a terrific bunch of resources on digital safety called **Feminist Tech Exchange (FTX)** Safety Reboot. Visit

http://en.ftx.apc.org/

for a curriculum made up of several modules for trainers who work with women's rights and sexual rights activists to use the internet safely, creatively and strategically.



Tactical Tech offers a large learning database under their Gender & Technology Manual on

https://gendersec.tacticaltech.org/

also developed collectively with several trainers from around the world.

The Internet Democracy Project in India works towards realizing feminist visions of the digital in society by exploring & addressing power imbalances in the areas of norms, governance & infrastructure. They offer a terrific resource on gender & surveillance online here

https://genderingsurveillance.internetdemocracy.in/

INSTITUTE FOR WAR & PEACE REPORTING

IWPR

The Institute for War & Peace Reporting offers an Arabic translation of a large cybersecurity manual on their resource website

https://cyber-women.com/