Input + activity: Online safety "rules" [deepening activity]

image-1605640472202.png
Image not found or type unknown

This learning activity is about sharing basic principles of online safety, and having the participants articulate personal or organisational policies to safeguard their online safety.

This activity can be done after Input + discussion: Privacy, consent and safety or Develop your internet dream place, and be the basis for Making online spaces safer.

There are three main parts to this learning activity:

- Input on the basic principles of online safety
- Reflection on communication practices
- Articulating "online safety rules".

Learning objective this activity responds to

- Come up with some strategies to create safe online spaces for themselves and their networks.

Who is this activity for?

Participants with differing levels of experience. However, note that participants with more experience with digital security might find this too basic.

Time required

105 minutes total (1 hour, 45 minutes):

- Input on Basic Principles of Online Safety (15 minutes)
- Activity on Communication Practices (30 minutes)
- Input on Areas of Consideration for Online Safety (20 minutes)
- Activity on Articulating "Online Safety Rules" (30 minutes)
- Debrief/Synthesis (10 minutes)

Resources needed for this activity

- Flip chart paper or white board
- Markers
- Printer paper

Mechanics

Start with listing down the **Basic Principles of Online Safety** (see Additional Resources)

> **Note:** It would be good to refer to examples that were shared in previous learning activities as you expound the principles.

Then move on to having the participants reflect on their communication practices by having them individually fill in this form (filled out a sample). To frame this, and to not conflate this activity, ask the participants to think about the last 24 hours and who they communicated with and what they communicated about.

Who do you communicate with	What topics you communicate about	Is the communication private?	Communication channels
Mother	My current trip	Yes	Facebook messenger
Kartika	Details of current work	Yes	Email, Telegram, Facebook messenger
Lisa	Event with them next month	Yes	Email
Marina	Dinner with him next week	Yes	SMS
	About how Trump sucks	No	Facebook group
	Feminist principles of technology	No	Personal blog

> **Intersectionality Note:** The names on the table are suggested names. You can change those names to fit in more common names in your country or context.

The starting point can be the people they communicated with, or the topics they communicated about in the last 24 hours.

After getting the participants to fill in their individual forms, have them reflect on the following questions:

- Of the communications that they had done in the last 24 hours, which of these do they think they should be securing the most?
- Of the communications that they have done in the last 24 hours, which one causes the most stress? Why?

Then move on to presenting the Areas to consider in online safety (see Additional Resources).

After, ask the participants to reflect on the areas to consider and write down their personal "online safety rules" based on this template:

- Which topics that you communicate about are private, and which are public?
- Who do you communicate with, and what about?
- Who are you permitting to have access to your communication channels?
- Which communication channel or device are you limiting access of others to?

> **Note:** These rules are draft rules and are personal to each participant. It is important to frame this activity this way, and keep on reiterating the Basic Principles of Online Safety.

After the participants have written down their "online safety rules", debrief on the activity:

- Insights on your communication practices?
- Any concerns that were raised because of this activity?
- What else needs to be clarified?

It is suggested that you then move on to Making online spaces safer.

Facilitator preparation notes

You might want to read this piece from Level Up: Roles and responsibilities of a digital security trainer to mentally prepare for this activity.

Additional resources

Basic principles of online safety

- The idea of perfect online safety is false. The security and safety scenario is contextual – it changes over time. What is safe today may not be safe tomorrow.
- Online safety must always be end-to-end. You are only as secure as the least secure person you communicate with, or the least secure platform you use.
- Online safety will always entail a combination of strategies, behaviour and tools. Merely installing security apps does not equal being safe online, especially if you have un-secure communication practice and behaviour.

> **Facilitation Note:** These may seem sanctimonious and might cause participants to feel paranoid about their safety. One way to go about this, as a feminist trainer, is to give examples that are personal to you and your experience. This way, the participants will not see you as someone who will judge them for their communication and digital security choices.

Areas to consider in online safety

These are areas the participants should be considering when they think about their online safety.

Who you communicate with and what you communicate with them about

- What topics do you talk about with the different people you communicate with?
- Are any of the topics you communicate about sensitive? How so? What are they?
- Are any of the people you communicate with at risk? Have they experienced surveillance? Is the work that they are doing a threat to someone with power?
- Are you at risk? Have you experienced surveillance?

What you use to communicate

- What platforms do you use? Do you know where they are hosted?
- What devices do you have?
- Do you use different devices for different people? Do you differentiate devices based on the public or private nature of your communications?
- Who has access to these communication channels? Are they shared?

Your specific context, capacity and risk

- Are there laws in your country that threaten your online safety as an individual? What are they, and how do they do this?
- Have there been examples of cases where individuals in your context (define that as you will) have had their online safety compromised? How?
- Have you ever experienced surveillance? From whom?
- Search yourself. Is there any information there that you don't want out in the public? Why?
- How do you safeguard your communication channels? Do you have passwords for each device and communication channel?

image-1605451259399.png
Image not found or type unknown

Revision #6
Created 16 April 2023 03:20:51 by Kira
Updated 28 July 2023 14:51:35 by Kira