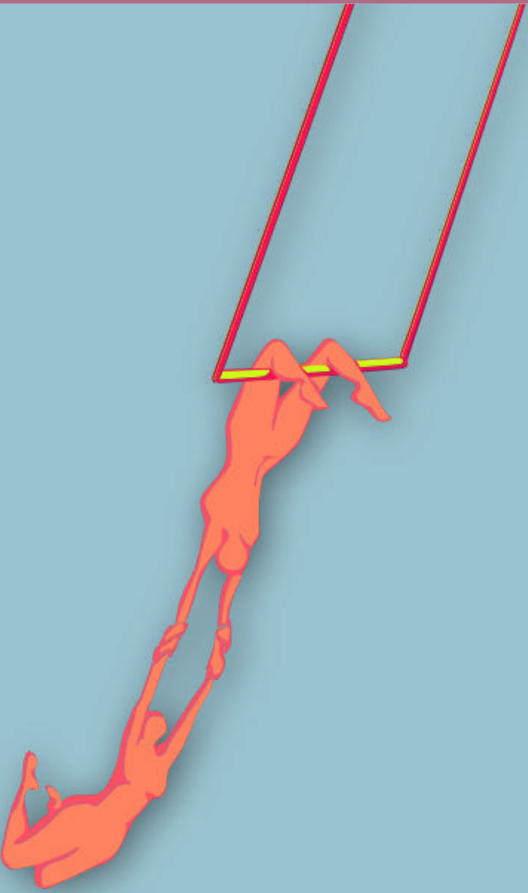
CYBERWOMEN



Trust-building exercises

Who do you trust?

Contents

1 Who do you trust? 5

Leading the exercise 6

Who do you trust?

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

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

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

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

- **Needed materials:**
  - Several large sheets of flipchart paper

Leading the exercise

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

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

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

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

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

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

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