CYBERWOMEN

Anonimity

More online identities!

INSTITUTE FOR
WAR & PEACE REPORTING

IWPR

Contents

More online identities!

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

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

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

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

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

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

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

  - Safe browsing[7]
- **Needed materials:**
  - Laptop/Computer and Projector setup
  - Flipchart paper (1-2 sheets per participant)
  - Markers or pens

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

Leading the exercise

Part 1 – Connected Online Identities

1. Begin the exercise by having participants make a list of any online identities they have; you may also simply ask the group if anyone among them currently uses more than one online identity. For any participants who indicate that they manage multiple online identities, ask them if they would be comfortable sharing their reasons for doing so with the rest of group and what they use them for.

2. Building off any examples shared by the group, explain that using multiple online identities is not an uncommon practice among WHRDs – offer some example scenarios:

   - WHRDs who use Facebook to manage online campaigns, but don’t want to use their personal profile or identity to administer the campaign’s page;

   - WHRDs who conduct sensitive research online, and want as few of the digital traces they leave behind to be traceable back to them;

you/

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

- WHRDs who have been documenting cases of government human rights abuses, and are planning to expose this information by publishing a major report or public statement.

3. Now ask participants to gather in pairs and identify other circumstances under which it might be useful for them to create a new identity that is not linked to their personal one. Have them reflect on how much they combine their personal identities with their activism work:

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

Part 2 – Separating and Managing Online Identities

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

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

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

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

- Separating professional from personal identities may only require users to change privacy configurations on their accounts, either to limit the amount of information that is available publicly, or to specifically manage what level of information is visible to specific friends, followers or contacts; in other cases though, separating these identities could imply the need to maintain entirely separated set of profiles and accounts for each (meaning that a new set would need to be created for either the personal or professional identity).
- Leaving an identity as it is would likely only require users to change privacy configurations on their accounts, either to limit the amount of information that is available publicly, or to specifically manage what level of information is visible to specific friends, followers or contacts.

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

Part 3 – Hands-On Practice and Recommendations

6. Explain to participants that they are welcome to choose any of the three options presented for the next part of the exercise (the steps below though will use the example of creating an entirely new identity).
7. Give each participant 1-2 sheets of flipchart paper and some markers,

and ask them to start drafting characteristics of their new identity – some specific considerations for them to think about include:

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

What would their interests and hobbies be?

Where are they from and where do they live?

What avatar or profile photo would they use?

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

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

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

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

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

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

Participants should not follow anybody friends, family or their organization using their new identities – this could very quickly allow anyone looking closely enough to draw a connection between that identity and its real counterpart;

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

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

References

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