CYBERWOMEN

Privacy

Privacy

https://iwpr.net/

Contents

Privacy

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

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

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

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

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

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

  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
- **Recommendations:** Some participants may become unsettled or upset by some of the information available about themselves online during the "self-doxxing" part of this session. if this happens, be sure to make plenty of time for the final part of the session where participants will focus on strategizing next steps in response to the information they find. participants should each have access to a device with an internet connection for the practical part of the session.

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

Leading the Session

Part 1 – Do We Truly Have Privacy?

1. Start the conversation by asking participants whether they think privacy truly exists or not. Then, ask them about their own concept of privacy - share your own concept of privacy to provide an example. Transition into the next steps by telling the group that, in this session and during this training, you will all be reclaiming **your right to privacy!**

2. Ask participants to share some examples of factors that could be interfering with the control they have over their data, personal information, and other elements. These could be personal practices, the platforms they trust with their information, the knowledge they have about the tools and devices they use, or the actions of others in their networks.

Part 2 – “Self-Doxxing”

3. Explain to participants what **Doxxing means** – essentially, it’s the practice of gathering a substantial amount of personal information about someone and then making it public (usually online). You should also explain how doxxing is sometimes used against people as a revenge tactic, and is often used to endanger, harass, or threaten activists and human rights defenders.
4. Tell the group that, in this part of the session, they will practice “self-doxxing” as a way to find out how much (and what kind) of information can be found about themselves online. Explain that this is useful preventative measure for taking steps to reduce the available amount of this information (when this is possible).
5. Ask participants to open a blank document on their computers, or to have a piece of paper ready to take notes of what information they discover. Then, have participants launch a browser window on their computers with a browser that is not the one they typically use – this is so they are not automatically logged-in to their various online accounts.
6. Ask participants, before they begin, to make a list of all the public accounts or social media profiles they have; then, ask them to make a list of keywords or phrases that could be linked to them, which could include information such as:
    - The city where they were born
    - The city where they currently live
    - Their home address
    - The organization they work for (or organizations they work with regularly)
    - Their activism cause
    - Major projects or campaigns they work on
7. To begin their self-doxxing, participants should first search for their various online accounts and profiles (these should appear as they would to the general public, since they won’t be logged-in), taking note

of what information about themselves they are able to find.

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

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

Part 3 – What Do We Do Now?

9. Explain to the group now that, through their self-doxxing, some may have found information about themselves that they didn't know was publicly available, as well as online accounts they don't use anymore which they may have even forgotten that they had.

10. Ask everyone to look back through the notes they took, and then to think about which next steps they could take to assert more control over what others can find out about them online. Have them each make a "to-do" list of these steps, which could include actions such as closing certain accounts, editing their information and/or privacy setting configurations on social media profiles, enabling private domain registration on their website domain hosting, etc.

11. As participants make their to-do lists, share with them some resources that could be helpful for them as they implement some of these next steps – they may also get inspiration for other steps they hadn't yet thought of:

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

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

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

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

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

References

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