CYBERWOMEN

Privacy

Apps and online platforms: friend or foe?

https://iwpr.net/

Contents

Apps and online platforms

- **Objective(s):** To focus on the apps and online platforms they use most – you will help them to identify the kinds of information shared with these platforms, and to strategize tactics for using them safely in their personal activities and online activism.
- **Length:** 120 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
  - Personal perceptions of security[1]
  - How does the internet work?[2]
- **Related sessions/exercises:**
  - Ask me anything![3]
  - Privacy[4]

[1] https://cyber-women.com/en/rethinking-our-relationship-with-technology/personal-perceptions-of-security/

[2] https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/

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

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

  - Networked publics[5]
  - Safe online campaigning[6]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
  - Paper (a few sheets for each participant)
  - Post-it Notes (in multiple colors)
- **Recommendations:** Participants should have their mobiles or one device with internet for the practical part of the session. provide participants with further recommended resources where they can learn more about privacy, and steps they can take to better protect theirs (see references section for links).

Leading the session

Part 1 – Our Devices, Our Data

1. Ask participants to go through all the apps they have on their devices and check the following:
   - Which device permissions each app has;
   - Their privacy policies, to see what can be done with the data each app has access to.
   - Who the developer of each app is.
2. Give participants approximately 15 minutes to do the above. Once time is up, ask participants to share what they found in this quick search. Make sure that you cover issues such as:
   - App permissions that have no clear relationship with their actual function;
   - Terms of Service that are unclear or vaguely written;

[5] https://cyber-women.com/en/privacy/networked-publics/
[6] https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/

- Privacy policies that allow companies to sell user data to third parties.

3. Share examples of "menstruapps" - menstrual cycle tracking apps - and other personal health related apps with the group. Explain how according to research that has been done (via Chupadatos[7]), it's been shown that menstruapps can gather quite a bit of personal data from users:

    - Name, phone number and address
    - Bodily details such as menstrual pain, weight, and hours of sleep;
    - Emotional states like stress, lack of concentration or anxiety;
    - Details about sexual health, including any contraceptive methods;
    - Online behaviors like click-throughs and type of devices used;
    - Offline behaviors including medicine taken, or habits like drinking or smoking.

That's a lot of information, right?

Part 2 - Who Else is Tracking Us?

4. Split participants into groups of 3-4 participants (maximum) and ask each group to make a list of what they know about Facebook and Google – to provide an example, you can have them start buy answering these questions:

    - Are these entities actually companies?
    - What are these companies' missions or objectives?
    - What are the services they offer?
    - Are those services for free or paid?
    - What are the rules/terms of those services?

    Give participants 15 minutes to finish listing all the information they have.

[7] https://chupadados.codingrights.org/es/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros/

5. Once time is up, ask each group to then make a list of what these two companies, Facebook and Google, might know about them. If participants have access to internet from their computers or mobile devices, those who have a Gmail account may want to visit the page https://www.google.com/maps/timeline as well to help with this part of the session. Give participants 20-25 minutes to make their lists, which each group should then briefly present to the rest of the participants.

Part 3 – Promoting Women's Rights Using Social Networks

6. For this next part of the session, keep participants in their present groups – you will give each group a question to discuss and work on together (taking from the list below):
    - Which tools or online platforms are we using to organize and exchange information from our social movements, protests and campaigns? What are some of the advantages or disadvantages of using those tools for that purpose?
    - Do we know any examples of censored campaigns, pages taken down from Facebook, videos censored on YouTube or other instances of social media accounts being closed?
    - Companies like Facebook and Google are good friends of our governments, and are known to share users' information with them (https://govtrequests.facebook.com) What are the implications of this?
    - Do we know of any cases of violence against women online? Specifically, any cases involving WHRDs receiving threats online, having their nudes exposed, or social media accounts being created to discredit them or "advertise" their sexual services? On which platforms did these incidents happen, and how did the platform react?
    - Have each group take about 10-15 minutes to answer their question; once time is up, ask each group to share their conclusions

with the rest of the participants.

7. Together as a group, take 5-10 minutes to reflect on how these same social networking platforms also serve as gathering places for many online users – as such, they seem to be ideal places to implement campaigning efforts. Ultimately, Facebook and the various services offered by Google provide different useful ways to interact with followers and community members; therefore, despite some of the concerns or disadvantages of these platforms, it's important to remember that many participants may still want to use them to reach out to their audiences.

Part 4 – Reclaiming Privacy

8. You'll now lead participants through the final closing portion of the session. Explain that you will now look at ways to reclaim privacy online, by learning how to continue using these apps, online platforms and social networking sites for personal use or advocacy efforts, but in a safer way.
9. With participants remaining in the same groups as before, ask them to now focus on collaboratively brainstorming creative ways to reclaim their privacy. Give each group a block of post-it notes along with some markers and pens, and have them generate as many ideas as they can think of in 10-15 minutes. You can provide some example tactics to get them started, such as:
    - Confusing the algorithms that platforms use for advertising or content optimization;
    - Regularly checking platforms' privacy policies and updates to privacy settings;
    - Being aware of app permissions on their devices, specifically things like location settings and geo-tagging of photos and posts;
    - Using alternative platforms that are more committed to privacy

and activism (Riseup, Tutanota, Signal, etc.)

Once they've finished this final part of the exercise, have each group share some of the ideas they came up with – you can post these in a visible place in the training room for participants to refer to as they move through the training process. These ideas will also be useful for you as you adjust the content of your training, especially if participants want to focus more on improving their safe use of social networks for their activism.

References

- https://www.kaspersky.es/blog/digital-detox-advices/6226
- https://rankingdigitalrights.org/2017/08/30/rdr-en-espanol-guest-post
- https://myshadow.org
- https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual
- https://www.digitale-gesellschaft.ch/dr.html
- http://www.europe-v-facebook.org