CYBERWOMEN

Online violence against women

Doxxing the troll

INSTITUTE FOR
WAR & PEACE REPORTING
IWPR

Contents

Doxxing the troll

- **Objective(s):** To introduce participants into a series of tools and activities focused on gathering information about their online harassers. this information can be used to help them make decisions in terms of privacy and security online.
- **Length:** 180 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
  - Safe browsing[1]
  - What does your metadata say about you?[2]
- **Related sessions/exercises:**
  - Safe browsing[3]
  - What does your metadata say about you?[4]

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

[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/safe-online-advocacy/what-does-your-metadata-say-about-you/

  - [Let's start a documentation journal!][]
- **Needed materials:**
  - Printed copies of the Documentation Journal Template (Online)
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
- **Recommendations:** This exercise is recommended for groups of whrds that are currently experiencing online harassment/online threats, or those who have very recently experienced these. though not explicitly required, this exercise works best if participants have already done let's start a documentation journal! this exercise works best if participants each have their own device or computer. you may want to split this session into two parts, as it is quite long and can be very intensive – you can also keep this as one session, but with a longer than normal break in the middle.

This exercise was adapted from an activity developed by Indira Cornelio (SocialTIC) and Phi Requiem (#SeguridadDigital) with the collaboration and support of APC's Take Back the Tech

Leading the exercise

Part 1 – What is Doxxing?

1. 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.

2. Highlight this important reminder for participants before continuing onward with the exercise:

   The goal of this exercise is not to recommend doxxing as a best practice (or to recommend using illegal or dubious methods of doing so) –

as doxxing implies the public release of personal information, it is important to highlight that ‘outing’ someone’s identity or information is not necessary. Rather, the goal of this session is to show participants how to gather this kind of information online to help them make informed decisions about addressing abuse or harassment.

3. Finally, explain also that it is important for participants to recall what they know about safe browsing practices – part of this exercise involved visiting harasser’s profiles and online spaces.

Part 2 – Identifying Harassers

4. Work with participants to set their expectations for the exercise, asking them - What do they want to find out about their harasser(s)? Mention several possible motives before participants begin sharing:
   - Is it to know their real identity?
   - To understand their motives for harassing them?
   - To find out if they are harassing other WHRDs as well?
   - To find out if it is just one person, or several people acting as one?
5. You may find that some participants have heard of ways to obtain this kind of information about their harassers, but make it clear to them that the tools and tactics you will be sharing have certain limitations. If the group has already done the Let’s Start a Documentation Journal! session, remind them of the importance of maintaining that body of evidence – it is critical for establishing patterns of abuse and for reporting harassment. If the group has not already done the Let’s Start a Documentation Journal! session, explain that later in this exercise you will review a method for keeping track of harassment incidents.

Part 3 - Different Profiles, Different Motives

6. Share a couple of cases of women activists or journalists and their experiences with online harassment. Try to find cases that are relevant

to the context of the participants, and that show different profiles of harassers and different motives for their actions.

7. Only if there are any women who feel comfortable sharing their own experiences with online harassment, ask them – About when did it begin? Who do they think the harasser is? Do they know them? Is there a specific motivation they can think of for their actions?

8. Reflect on possible motives that their harasser might have - Is the harassment happening because they are a women? Because they defend women's rights/human rights? Have they seen this kind of harassment against their male partners or colleagues? If so, does it happen the same way or differently?

Part 4 - Documenting Incidents & Threats

9. If participants have already gone through the Let's Start a Documentation Journal! session, review the key takeaways with participants once more and explain how a documentation practice is an important part of gathering information about harassers to make decisions about next steps and actions. You can then skip down to Part 5 – Getting Ready.

10. If participants have not yet gone through the Let's Start a Documentation Journal! session, start out by first explaining the following points, which highlight why documentation is an important practice for addressing online harassment:

    What is Documentation?

    Documentation in this context refers to a systematic, organized approach for keeping a track of any incidents of abuse or harassment that occur in the course of our work – essentially, it is maintaining an archive of evidence.

    What is an Incident?

    An incident is anything that happens either online or offline that might constitute abuse or harassment – whether an event can be classified as an incident or not is highly dependent on the context and circumstances in which it happens, and the severity of its impact in relation to those. For example, if you receive an email that seems like a phishing attempt – and you're used to receiving these every so often – that alone might not be significant enough to be an incident; however, if your organization is about to launch a major campaign, and you begin receiving an unusually large number of these emails, this would likely constitute an incident (and it should be documented). To provide another example, the same could be said if your organization is about to launch a major campaign and you begin receiving usually large numbers of Facebook friend requests from strangers.

What is a Documentation Journal?

A documentation journal is a place where you can keep records of incidents that occur, in an organized way that will help you save important information and evidence from each for later use or reference.

Why is Documentation Important?

Documentation can be useful for later reference when attempting to connect the dots between different incidents that took place during a specific timeframe, or that happened to several people in the same organization. Documentation can reveal patterns of abuse or other online attacks you may not have otherwise noticed, by presenting a collated body of evidence – these patterns can be helpful for identifying adversaries, or to draw connections between certain kinds of incidents and certain actions of yours or your organizations. When reporting incidents of abuse on social media platforms, for instance, evidence such as screenshots or profile names may be requested during an investigation.

11. Now, you can introduce the Documentation Journal to participants – for this exercise, you can just use the Online version, which you should have printed versions of prepared to hand out to the group – see the template below:

Documentation Journal Template (Online)

Date
Time
Summary of incident
Platform
URL
Screenshot (filename or copy/pasted)
Description of screenshot content(s)
Risk level
Follow-up actions
Notes

12. Mention to participants that this template provides just one example of the kinds of information that could be important to gather when gathering information about harassers. They should feel free to add or remove columns and fields as they see fit when creating more specific formats that are relevant to their context.

13. Most of the fields in these templates are relatively self-explanatory; however, you should still walkthrough each one for the group, describing briefly to what each one refers (in terms of what participants should be keeping track of for each).

14. Be sure to specifically highlight the Level of Risk field, as this field is highly subjective and less self-explanatory than the others. How different participants and/or organizations define levels of risk will be extremely specific to their context – it might be useful to pause at this point and ask participants for examples of incidents they would define as Low Risk, Medium Risk, or High Risk (for instance). Emphasize to participants that they should consider the potential impact of the incident (on either a personal or organizational level, or both) when defining risk in this context.

15. Ask participants to begin filling in their journal templates individually

- give 10-15 minutes to fill in as much as they can. Although they can fill in the details of actual incidents that have occurred if they wish, participants can also use hypothetical examples for practice purposes.

Part 5 – Getting Ready

16. Before moving on to the next steps in the exercise, for participants to be careful not to click on any link they might receive or find while doxxing their harasser – these could be possible phishing attempts (explain what this is if participants are not familiar) that could install malicious software on their devices. Highlight that its extremely important to avoid providing additional information about yourself to harassers; likewise, for participants going through this exercise who are not currently experiencing online harassment, they will want to avoid attracting unnecessary attention to themselves that could lead to later harassment:

17. Walk participants through the following steps to safely begin gathering information about their harassers:

    - They should collect any information they may already have on hand about their harassers (or document any past incidents they can recall in their documentation journals);
    - Then, they should choose the browser they will use for their investigation – on that browser, they should logout from any of their accounts, and erase their browsing history and cookies. They may want to consider using Tor Browser for this activity, if you have already covered this with them;
    - They may also want to consider creating new online identities or profiles to perform this activity (such as an alias Facebook or Twitter account, or a fake Gmail account) – remind them to be careful not to use any information for these accounts that could be used to link back to their real identities!

- Emphasize the importance of taking notes during this process – remind the group of what you discussed when addressing the importance of documentation practices.
- Have participants create a dedicated folder on their computers to gather and store any information or evidence they collect – these could be avatar images, screenshots, user names, email and social media accounts, comments on forums, or mentions of their possible locations or other known contacts.

Part 7 – Useful Tools

18. Now you can start sharing examples of tools that will be useful to participants during their doxxing investigation - if possible, provide participants a copy of your presentation containing this information, or a handout with the tool list and links that they can refer to later on their own.
19. Explain each of the tools, giving participants a few minutes for each to locate them online and try them out (aside from those included here, feel free to add any others you know of that could be useful or relevant):
    - Google searching, or Duck Duck Go[5];
    - Advanced search on Twitter[6];
    - Checking Whois.net in case they can find information that comes from a website to see if there is any information about who owns the domain;
    - Google reverse image search[7] in case they have received images or photos they can do an image search;
    - Metadata tools in case they have received images or photos they can see if there is any metadata available:

[5] https://duckduckgo.com

[6] https://twitter.com/search-advanced

[7] https://images.google.com/

- MetaShield[8]
- MetaPicz[9]
- Social Mention[10];
- Follower Wonk[11];
- NameCheck[12];

20. Explain also that there are ways for participants to build mini-monitoring systems for tracking information online: this works well for tracking certain profile name, username or hashtag:

    - IFTTT[13] – for IFTTT, explain how it allows users to connect Twitter with Google Drive to keep track of tweets and mentions connected to a certain username or hashtag.
    - Google Alerts[14]
    - Tweetdeck[15]

21. Depending on how much time you have available, participants can either do their investigations now during the workshop, or they can do them as "homework" for the next training day. Either way, remind the group that it will be helpful – once they are done collecting information – to take a step back and look at everything they have gathered:

    - Do they see any patterns emerging?
    - What does the information they have tell them about who their harasser might be?
    - Perhaps they can even predict potential future targets or kinds of attacks?

[8] https://www.elevenpaths.com/technology/metashield/index.html

[9] http://metapicz.com/

[10] http://socialmention.com

[11] https://moz.com/followerwonk/

[12] https://namechk.com

[13] https://ifttt.com

[14] https://www.google.com/alerts

[15] https://tweetdeck.twitter.com

References

- https://summit2015.globalvoices.org/2015/02/do-we-feed-the-trolls-learning-from-our-community/
- https://citizenevidence.org/category/how-to-2/tutorials/