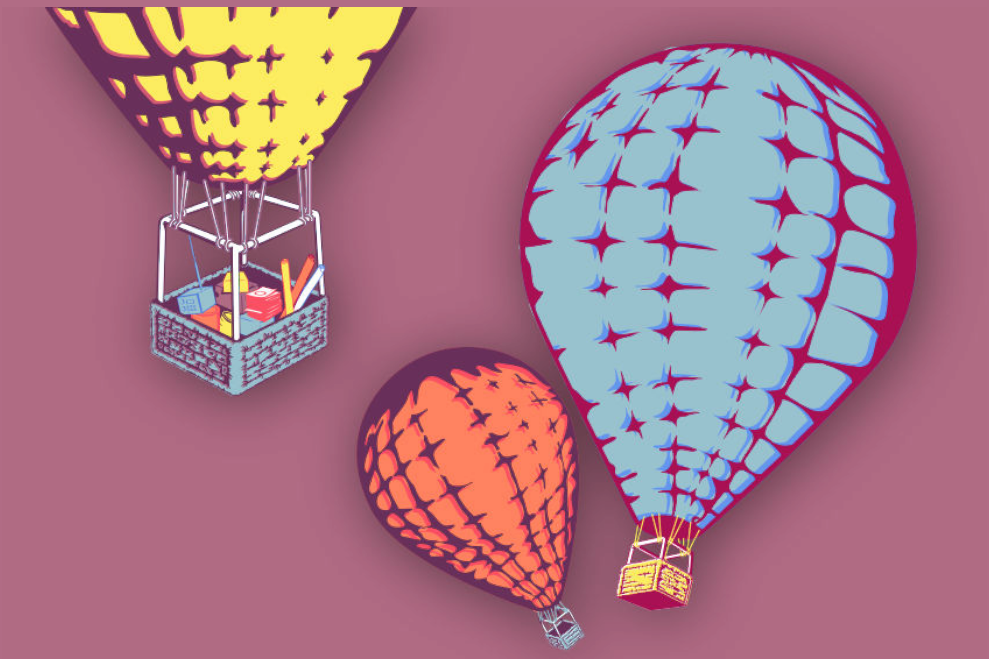
CYBERWOMEN



Safe online advocacy

Safe online campaigning

https://iwpr.net/

Contents

1 Safe online campaigning **5**
Leading the session 6
Part 1 – Introduction and Preventative Planning 6
Part 2 – Protecting Devices 7
Part 3 – Managing Account Access 8
Part 4 – Choosing Apps for Campaigns 9
Part 5 – Community Building through Facebook 10
Part 6 – Informed Consent 11
References 12

Safe online campaigning

- **Objective(s):** To share digital security recommendations for women human rights defenders who are involved in online campaigning efforts.
- **Length:** 50 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Who do you trust?[1]
- **Related sessions/exercises:**
  - Who do you trust?[2]
  - Gender-based risk model[3]
  - Apps and online platforms: friend or foe?[4]
  - Safer websites[5]
  - Building stronger passwords[6]
  - Malware and viruses[7]

[1] https://cyber-women.com/en/trust-building-exercises/who-do-you-trust/
[2] https://cyber-women.com/en/trust-building-exercises/who-do-you-trust/
[3] https://cyber-women.com/en/determining-the-best-solution/gender-based-risk-model/
[4] https://cyber-women.com/en/privacy/apps-and-online-platforms-friend-or-foe/
[5] https://cyber-women.com/en/safe-online-advocacy/safer-websites/
[6] https://cyber-women.com/en/digital-security-basics-1/building-stronger-passwords/
[7] https://cyber-women.com/en/digital-security-basics-1/malware-and-viruses/

  - How to secure your computer[8]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
- **Recommendations:** The intention of this session is for participants to identify digital security solutions they can implement for safer online campaigning activities; however, the ultimate goal is not for them to implement these during the session, rather it is for them to begin a process of exploration to identify what will work best for their individual context.

This session is based on a guide developed by Indira Cornelio for SocialTIC.

Leading the session

Part 1 – Introduction and Preventative Planning

1. Explain to participants that the intent of this session is for them to identify digital security solutions they can implement for safer online campaigning activities. They won't need to immediately implement these during the session, however - the goal is for them to begin a process of exploration to identify what will work best for their individual contexts and campaigns.
2. Ask participants to share any examples of online campaigns they are aware of – are there any emerging trends in how these campaigns are implemented that they can identify?
3. Remind participants that, when it comes to mounting their own online campaigning and advocacy efforts, they should keep in mind the information and adversaries they identified during the Who Do You Trust? exercise. As campaigns are, by nature, very public efforts, they should

[8] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/

be extra aware of who could potentially be monitoring them, or who might potentially pose a threat to them.

4. In the context of their own work, suggest to participants that when it comes time for them to begin the planning phase an online campaigning effort, they should work with their team(s) to answer the following questions:
    - What is the campaign about?
    - What is the key audience? How do they feel about the topic or issue? Are they for or against it?
    - Who might feel targeted or exposed by this campaign?
    - What are potential arguments that could be made against this campaign?
    - What are the best and worst-case outcomes for this campaign?
5. Answering these can help them plan preventative measures against possible threats more strategically – highlight to the group that they can even prepare messaging in advance for possible scenarios that emerge from the responses to these questions. Also, remind participants that even envisioning the best-case scenario of the campaign is helpful for planning preventative measures – for instance, how would they prepare for the possibility that, if the campaign is successful and becomes quite popular, their website is unable to handle a sudden surge in traffic and goes down?
6. Now, explain to the group that during the next parts of this session, you will be providing guidance and recommendations on digital security practices useful for online campaigning efforts (if possible, depending on how much time you have to work with, allow participants to visit recommended tools' websites).

Part 2 – Protecting Devices

7. Ask participants if they use their own personal devices for campaigning (versus a "work" device) - how much campaign related information

they store on these devices? Are they connected to email and social media accounts as well?

8. Here are some topline practices to recommend to the group for device protection:

    - **Password-protecting** their laptops and mobile phones;
    - **Installing antivirus software** on both laptops and mobile phones;
    - **Performing regular backups** of important or sensitive data (recorded video or audio, interview notes, reports, etc.) with the backups kept in a safe location separate from their devices;
    - **Enabling full-disk encryption** of their devices:
        - For Android and Mac iOS mobile devices, this can be enabled via phone settings;
        - For laptops, Mac OSX FileVault[9] and Windows BitLocker[10] are the most common options for full-disk encryption;
        - Note: Filevault comes for free with Mac OSX; however, BitLocker only comes free with Pro, Enterprise and Education versions of Windows.

Part 3 – Managing Account Access

9. Online campaigns often require multiple users to be able to access the same online accounts (or devices, in some cases). Access to a device or account by multiple users with the same credentials represents a significant increase in risk; however, by taking some preventative measures, participants can substantially reduce the likelihood of these risks becoming direct threats:

    - For all shared online accounts and devices, limiting the list of those with access to as few people as possible is among the most critical first measures to implement; another is to make sure that any protocols or procedures put into place (especially regarding

[9] https://en.wikipedia.org/wiki/FileVault
[10] https://en.wikipedia.org/wiki/BitLocker

the following recommendations) are followed **regularly and consistently**;

- For online platforms in particular, all team members with access should make sure to regularly check history and activity on shared accounts – for example, on Gmail/Google accounts, they can check the history of recent log-ins (and set alerts for suspicious activity) under "Last Account Activity"; likewise, for Facebook, they can go to the shared account's Activity Log to check on recent activity;
- Apply basic strong password practices for all devices and accounts that will be used for a campaign. Secure password storage managers like KeePass/KeePassX[11] allow individual database files of account passwords to be created, which are in turn protected by a master password; likewise, for accounts like Google, Facebook and Twitter, enabling two-factor authentication provides an additional layer of access control and is highly recommended;
- If a password needs to be shared between team members, but can't be done in person, sending passwords over encrypted email - with GPG or using a service like Tutanota[12] or over encrypted messaging (using Signal on a mobile device) are safer options – if using Signal, make sure to set a protocol with team members about deleting messages with passwords from their devices as soon as they are received.

Part 4 – Choosing Apps for Campaigns

10. When implementing and organizing an online campaign, it is common to use certain apps and tools to keep track of social media/website metrics, or to schedule social media posts. When making decisions about

[11] http://keepass.info/
[12] https://tutanota.com/

such apps, and which ones to use, there are few questions that participants should keep in mind – these are primarily for them to avoid sharing their information with certain unsafe tools, or tools that are no longer supported by developers:

- Is the app still active, with developers pushing regular security and feature updates?
- Does the app have social media accounts that can be followed and interacted with?
- What are other users saying about the app online and on their social media channels?
- Are there any recent blog posts available about the app?

Part 5 – Community Building through Facebook

11. Facebook is often used in online campaigns to organize communities and to quickly disseminate important messaging and other communications. It is important, however, to highlight some of the potential vulnerabilities are with using these platforms as part of a campaign's core organizing structure:

- Participants should be aware of the implications of using Facebook (or other large social media platforms) could be for their own identities online – to limit their exposure, they should create dedicated profiles specifically for administering pages, rather than using their own personal profiles;
- Note, however, that it is now possible to receive Facebook notifications that are encrypted using a public GPG key to an associated email account – this can be useful for WHRDs who want to take further measures to separate their work and personal identities online while managing campaigns;
- Those who are managing campaigns online should be very deliberate about the kinds of information and communication they share with online platforms like Facebook - there are past examples of campaign

Facebook pages and profiles being infiltrated by adversaries, making it necessary for administrators to close them down (or, pages are forcefully shutdown by the platform because of reporting by adversaries)

- This could represent a significant setback to campaign and community building progress, so highlight to participants the importance of having **alternative communication and organizing channels** – these could include:
  - Developing active communities on other platforms simultaneously, so there is always a backup platform to fall back on;
  - Users can also download a Facebook page's information to create offline backups, which is a good strategy;
  - Using a service like Riseup lists[13] to create email groups for sending out newsletters and other communication;
  - Organizing in-person meetups if possible; however, for campaigns addressing certain issues in certain countries, be aware that this may be extremely risky and therefore not advisable;

Part 6 – Informed Consent

12. Discuss the importance of informed consent with the group – this is important generally for awareness raising campaigns on human rights issues, and especially when using images or testimonials of victims, survivors and witnesses of atrocities or other violations in campaign materials:

- Before recording images or video of these individuals, or documenting their stories, they must have explicitly agreed to this beforehand; likewise, they must also explicitly agree to having any of this material **shared publicly** – it should furthermore be made clear to them where and for what purpose these materials will be shared, and what the potential implications could be for them.

[13] https://www.lists.riseup.net

References

- http://seguridadigital.org/post/156287966318/consejos-de-seguridad-digital-para-gestionar-redes
- https://archive.informationactivism.org/en/index.html