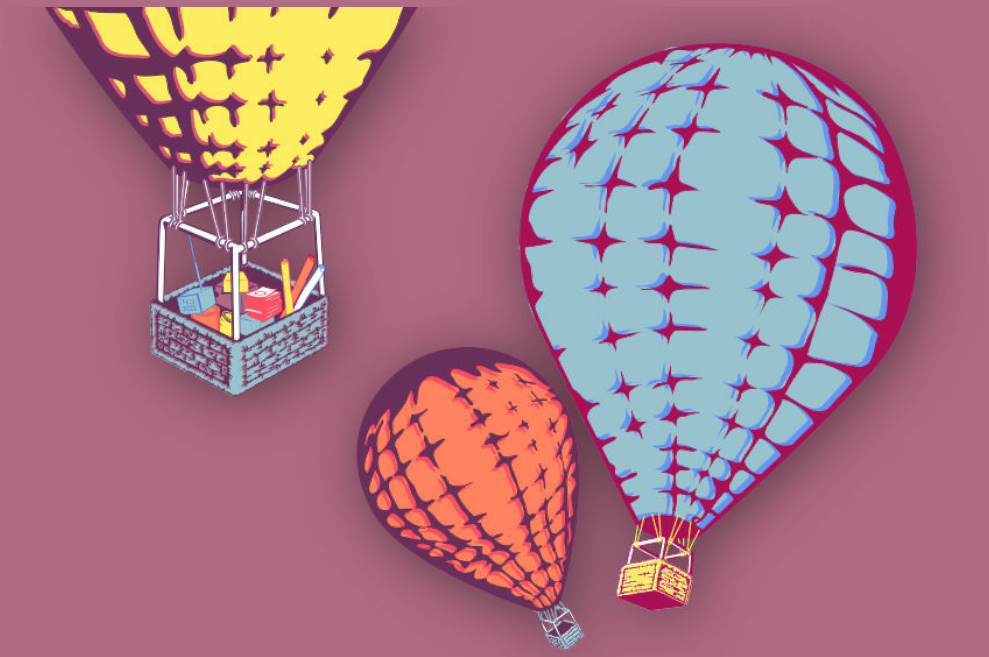
CYBERWOMEN



Safe online advocacy

Safe online advocacy

https://iwpr.net/

Contents

Safer websites

- **Objective(s):** To help whrds to identify safer practices to implement for managing and protecting their websites – these could be personal websites that they use for online activism, or the websites of their organizations/collectives/movements.
- **Length:** 50 minutes
- **Format:** Session
- **Skill level:** Advanced
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
  - Familiarity with how websites are administered
  - Who do you trust?[1]
- **Related sessions/exercises:**
  - Who do you trust?[2]
  - Apps and online platforms: friend or foe?[3]
  - Safe online campaigning[4]
- **Needed materials:**

[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/privacy/apps-and-online-platforms-friend-or-foe/
[4] https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/

  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
- **Recommendations:** This session will be more relevant for some groups than for others - prioritize this session especially for women activists or collectives that have a website. it may be a good idea to prepare ahead of this session a few examples (from news reports, blogposts, social media postings or personal experience) of online attacks against whrds and/or whrd organizations, websites hacks or takedowns in particular. remember that in some cases, organizations may not manage their own websites, or their ability to make changes to their websites might depend on the decisions of larger international ngos who support them. either way, even if participants are not able to directly make changes to the processes for administering their websites, this session still provides a solid foundation for them to begin thinking about changes that they might propose (or taking more control over managing their sites).

Leading the session

Part 1 – What Does an Online Attack Look Like?

1. Begin the session by reviewing some of the responses provided during the session Who Do You Trust? (Trust-Building Exercises) – in particular, mention some of the possible adversaries identified by participants. This will provide a useful backdrop for addressing the issue of website safety, especially for women activists in online spaces.
2. Ask participants - What do they consider as an online attack? What are some of the cases of online attacks they have heard about? If appropriate, you may also ask if anybody in the group has been attacked in the past, either individually or in the context of their organization/collective. You can also offer some of your pre-prepared case studies in case participants don't have any examples of their own

to share.

3. Pose follow-up questions to the cases that participants (or yourself) have shared - Did the attack happen in the context of a specific event such as a protest, report presentation or another kind of public gathering? What was the response to the attack by the WHRDs involved? Was any documentation of the attack created?

Part 2 – Protecting and Securing Websites

4. Based on the examples participants have shared, you can now begin to share in turn some initial practice recommendations for improved protection of their websites. Some examples are included below - based on the different levels of knowledge within the participant group, you may want to offer more in-depth explanations for each of these:

   Optional: Even for participant groups equipped with some level of knowledge or information about managing websites, before moving on to the below recommendations it may be a good idea to explain the ways in which a website can be administered. Some example topics to mention might include domains and DNS, site hosting, and content management systems (CMS).

Protecting your website

- Use a strong admin password to avoid a website being hacked – adversaries taking advantage of weak passwords to access a website's backend is the most common way that hacking occurs. If possible, activate two-step verification for a website's account, hosting service, and any other portals of access.
- When a domain name is registered, it often requires that person registering it provide information such as their name, address and email. Check to see which information is available on a given domain registration, and consider changing it to a private domain registration (using

whois.net is an easy method for checking this).

- Where geographically is a website's domain hosted? There are several things to take consider in this regard, especially:
  - In which country (or even city) are the host's servers located? Can the government of that country be trusted with your data, and more importantly, can the hosting service be trusted not to hand your data over to a government's request? Could the government of that country attempt to interfere with or attempt to take down a website?
  - Consider if buying your host with the reseller of a reseller is a good option, in some attacks you will need to have a good support team that can help you, so make sure to choose well. Make sure to check that, as some of the hosts options can be well known for having a bad technical support.
- Check the plug-ins that a website currently uses – these are especially common on websites which use Wordpress as a CMS. Be sure to use only the plug-ins that are necessary, and check that any plug-ins currently in use are from a trustworthy source.
- Consider installing utilities like Jetpack by Automattic on WordPress, especially for services like social media widgets, comments and contact forms. There are also basic site security plug-ins available such as Better WP Security[5], as well as plug-ins for automatic data backup such as VaultPress[6] or Backup Buddy[7].
- Make sure to regularly perform updates to a website's hosting servers (if these are not automatically managed by the hosting service), as well as any updates to the CMS, plug-ins, or any other platforms that are used for administration and management.

[5] https://wordpress.org/plugins/better-wp-security/
[6] https://vaultpress.com/
[7] https://ithemes.com/purchase/backupbuddy/

Protecting your website's visitors

- It is highly recommended that websites offer HTTPS connections to users by default (not just as an option) – Let's Encrypt by the Electronic Frontier Foundation is a service that acts as a certificate authority and offers HTTPS certificates for no cost.
- There are many collectives in operation around the world that support tech activism efforts, and specialize in working with activist organizations - in Latin America for example, Código Sur and Kefir.red are options. Other similar collectives are Austisticy, No blogs and Blackblogs.org.
- If an organization or website has experienced Distributed Denial of Service (DDoS) attacks in the past, consider using the DDoS protection services offered by initiatives such as Deflect or Project Shield. Deflect, which is run by Montreal-based non-profit Equalit.ie, is a completely free service widely trusted in the digital security community.

  Optional: Consider sharing resources about responding to a DDoS attack, such as: https://github.com/OpenInternet/MyWebsiteIsDown/blob/dev/MyWebsiteIsDown.md

References

- https://onlinesafety.feministfrequency.com/en/
- https://www.apc.org/
- https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/en

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

What does your metadata say about you?

- **Objective(s):** Introducir el concepto de metadatos y la importancia de tomar conciencia sobre qué metadatos contiene cada tipo de contenidos, especialmente cuando estamos trabajando en situaciones de riesgo en el ámbito de derechos humanos.
- **Length:** 90 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Networked publics[1]
  - Safe online campaigning[2]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup

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

  - Example tools for analyzing and removing metadata
- **Recommendations:** While not required, this session is greatly enhanced for participants if they have already done the networked publics session. metadata is often one of the more complex topics to introduce in the training process - make sure to budget sufficient time to cover this session in detail, as it is quite critical and relevant to the context of whrds and women activists.

Leading the session

Part 1 - What is Metadata?

1. Begin the session by sharing a few key points with participants – the most important of these are included below:
    - Share a definition of what metadata is, and some common places where participants might encounter it (image files, Word/Excel documents, etc.)
    - Share a few common examples of metadata (date and time of creation, location created, username or author's name, type of device) – you may have participants locate an image or other similar file on their own computers so they can locate its metadata for themselves, or you can share some example screenshots of metadata as it appears in common file formats.
    - Explaining some of the different ways that metadata is created, and how it can be changed or even removed entirely.

    Metadata is often one of the more complex topics to introduce in the training process, so make sure to ask the participants if the concept is clear – if not, take time to answer their questions thoroughly and in detail based on your expertise.

Part 2 - Implications of Metadata in a Human Rights Context

2. When working with WHRDs, it is important to explain what are the pros and cons of metadata – you can succinctly describe this to participants using two key ideas:

   Metadata can say a lot about you.

   - Ask participants to take a picture with their phones and to check all the metadata that the image file contains - you will need to provide them with a tool such as CameraV to do this, or you may also share a web-based tool like http://metapicz.com if your training is with a very beginner-level group.
   - Now, have participants repeat the exercise but with location services disabled on their phones. Split participants up into groups of 3-4 people (maximum) to discuss how they think metadata could be useful, and how they think it could compromise security when performing human rights work.
   - In their discussion, keeping the focus on human rights work, it is important that participants also identify under which circumstances metadata found in documents, videos or images help such content be considered as evidence in human rights documentation work. Share with them some practices - such as saving the original files on an encrypted device and creating separate copies for editing or for storing on their computers.

   Metadata is created, but can also be removed.

   Share with participants a few options, such as ObscuraCam or Metanull, for erasing metadata from videos and images. If there is enough time left for the session, you might also consider including the option of erasing metadata from documents with LibreOffice.

References

- https://ssd.eff.org/en/module/why-metadata-matters
- https://guardianproject.info/apps/obscuracam/
- https://archiving.witness.org/archive-guide/create/how-capture-metadata/
- https://securityinabox.org/en/lgbti-mena/remove-metadata/