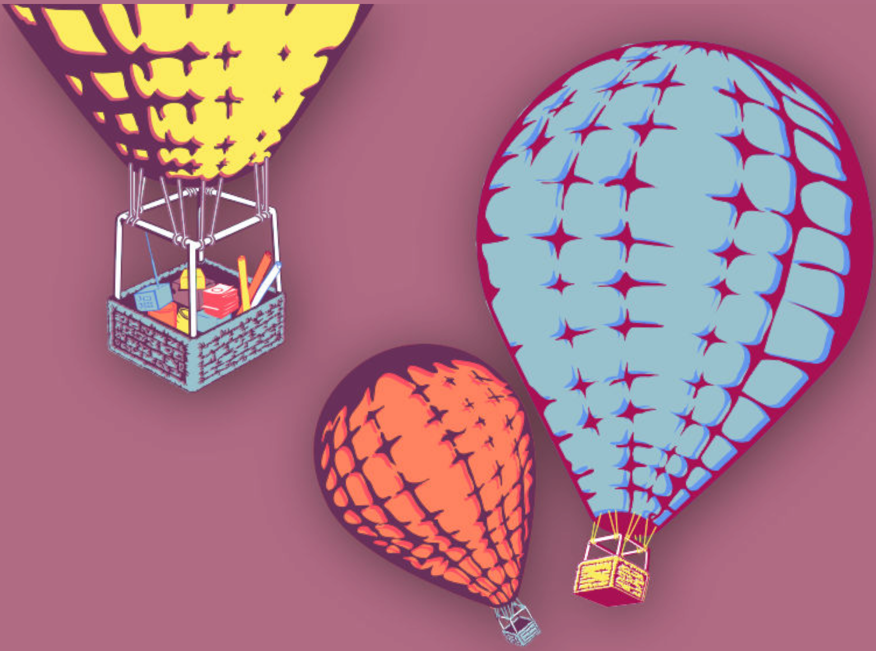
CYBERWOMEN



Safe online advocacy

Safer websites

Contents

1 Safer websites 5

Leading the session 6

Part 1 – What Does an Online Attack Look Like? 6

Part 2 – Protecting and Securing Websites 7

References 9

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