Designing Websites to Increase Survivor Safety and Privacy

Visiting a website can leave a digital trail and, for survivors, can create safety and privacy risks. A primary risk for survivors is that someone else may discover that they were seeking information or reaching out for help online. An abusive person, friends, family members, co-workers, or fellow students could know what a survivor is looking at online by either looking over their shoulder or reviewing the web browser history.

While it may not be possible to completely eliminate risks, through web design and by including content on safety and privacy, you can increase survivors' awareness and provide options. Below are tips to help minimize the safety and privacy risks on your program's website.

1. **Add a safety alert.** A safety alert should include a warning that visiting this or any other website, or simply searching for terms like "domestic violence" creates a digital trail that cannot be completely erased. A safety alert should inform the person of the risks and give them a chance to decide whether to continue or to leave. A header should also be at the top of every webpage because survivors may not start on the homepage. For example, check out the safety alert header on NNEDV's website or the safety alert pop-up window on the National Domestic Violence Hotline's website.

   Information to include:

   1. Other ways to seek help, such as emergency services, your hotline, or a national hotline.
   2. An option to leave the site quickly using a "Quick Exit Button" (more information below) or to close the browser window by using keyboard shortcuts such as Alt+F4 (Windows), or Shift+Command+W (Mac).
   3. Options for minimizing the digital trail by using safer devices and browser privacy options. You can **link to or copy our internet safety**

page and include a link to additional information about technology safety and privacy in our Survivor Toolkit at TechSafety.org.

NOTE: Don't give a false sense of security. If any of your web content discusses clearing the digital trail, also include information about the risks of spyware and device monitoring. Spyware, also called Stalkerware, monitors all activity, including attempts to delete browsing history. Read more about Spyware and Stalkerware.

2. **Include a Quick Exit button** that redirects the web browser to a reliable website, with neutral content (such as the weather or the news), that can load quickly. A Quick Exit button does not delete the current website from the browsing history, but it can be an option for a survivor to quickly pull up another website if someone enters the room when they're visiting your site.

   Another option is to code the button so that when it is clicked it re-directs to many websites in rapid succession to hide your website deeper in the browser history. The benefit of this is that if someone hits the "back" button, they won't go to your site; adding an additional layer or protection and privacy. The downside is that this will take longer to load, and still won't remove the browser history.

3. **Increase Safety & Privacy via "Contact Us" and "Find Help" Options.**
   - **Use clear visual cues and plain language** to direct survivors to the safest and most secure ways to contact you.
   - **Encourage survivors to reach out through your hotline**, and any other safer and more secure options you offer (e.g. text, online chat, etc.). Visit our Digital Services Toolkit for more information if you are considering starting new services.
   - **Remove email addresses from your website and use web forms instead.** For survivors reaching out to your program, hotlines and online chat are generally safer ways to communicate. However, web-based

contact forms are usually a better option for survivors compared to email. With a web form, the survivor's message goes through your website instead of through the survivor's email account, where a sent message could be found. On the web form, it is important to include questions about how your organization can safely respond. See Safety Net's Contact Us form as an example.[1]

NOTE: Email and social media are generally not secure or confidential ways to communicate. While we encourage programs to respond to survivors no matter how they reach out, be sure to offer other more secure options both in the design of your website, and after you connect with a survivor after they reach out.

4. **Use HTTPS.** HTTPS encrypts the data shared between the user's browser and your website, but it will still show in the user's web browser that your website was visited. HTTPS also won't protect against spyware or keystroke logging. Configuring your website for SSL/HTTPS has the added benefit of improving your rankings in search engines. Ask your website's host to add a SSL certificate if it doesn't already have one.

5. **Be Cautious with Third-Party Tools.** Sometimes called add-ins, plug-ins, or widgets, these third party tools might offer to add comments sections, maps, images, weather, or other features to your website. Some of these tools are designed to gather information about everyone who visits your site, and can pose a serious privacy risk.

6. **Links, including embedded videos and pdf documents, also leave a digital trail.**

1 Web forms are also helpful to your program because they reduce spam emails sent by automated technology that harvests emails from websites, and because you can better route inquiries from visitors other than survivors, for example people looking to ask about volunteering or requesting an expert speaker.

- Inform survivors that links to external videos will be both in browser history, and in the account history. For example, a video embedded from YouTube will be in browser history and their YouTube account viewing history. An alternative is to embed the video in your own site.
- Inform survivors that downloading a pdf from your site will place the document in their download folder.

Program Confidentiality

Websites can also pose challenges to programs' confidentiality obligations if they are set up in such a way that collects Personally Identifying Information (PII) about site visitors. Some basic website data, such as IP address, can be personally identifying. As with all other work with survivors, collect the minimum amount of information necessary to provide the information or services they are requesting. Read more in our Confidentiality Toolkit.

Below are options to minimize or eliminate the collection of identifying or potentially identifying user information.

1. **Don't use cookies.** Cookies are bits of code that track users' visits to your site, and sometimes the history of other sites they visit. If your website uses cookies, explain why it uses cookies in your privacy policy.

2. **Obscure the IP addresses of visitors to your site.** IP addresses can be personally identifying, and are usually stored by default for most websites. Techniques like Cryptolog mix up the IP address with other random information and encrypt it all, protecting the privacy of visitors to your site.

3. **Be selective with analytics.** Consider not using third-party analytics. Instead, use only the information you can glean from the webhost's server log. If you must use third-party analytics, customize settings to minimize the possibility of collecting identifying information. Inform users about any third-party analytics you use and provide information about how visitors can opt out of analytics on

your site through your privacy policy. You can also use a tool like this one that integrates with your website.

4. **Get informed consent for names, photos, documents, and videos that you post to your website.** This includes presenters, donors, board members, staff, volunteers, and other individuals whose information you publish (including in emailed newsletters). Remove any content that your organization does not have explicit consent to post. In addition, before uploading photos to your website, remove geotags from the digital file. Geotags add information about the location where a photo was taken. For example, a photo inside a confidential shelter might reveal the exact location if it was taken with a device with the location or geotag feature on.

5. **Provide clear information about your privacy policies.** This should include information on what data your site collects, who has access to that data, and how you use it. For more information, see our guide to Privacy Policies and Terms of Service. You can also analyze your current policies with this tool.

Ensure Accessibility

Programs should ensure that all people can access your website. Read more at the Web Accessibility Initiative's Tips for Getting Started with Web Accessibility.

 This product was supported by cooperative agreement number 2019-V3-GX-K017, awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this product are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice. We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.