Technology Safety and Your Website

1. **Add a safety alert header to your website.** Have it at the top of every page on your website, because you never know which page a survivor will visit first. For examples, check out the safety alert header on NNEDV’s website or the safety alert popup box on The National Domestic Violence Hotline’s website.

   Include an ESCAPE button that links to a reliable website that loads quickly (such as the weather or the news), redirecting the web browser to a less risky content. An Escape button does not delete web browsing history, but it can be an option for someone to quickly switch to a random webpage if someone enters the room when they are visiting your site.

2. **Add a link from your website to NNEDV's internet safety page.** You may also copy or adapt Safety Net's internet safety tips for posting on your own website (please still cite or link to the Safety Net Project and TechSafety.org).

3. **Don't have content that tells survivors they can safely clear or hide their online tracks without recognizing remote spyware tools.** If any of your website's pages discuss clearing internet history or tracks, make sure they also mention the risks of spyware and computer monitoring. If someone is using spyware, they will know all activity, including any attempts to delete browsing history. See our Spyware handout for more info.

4. **Remove email addresses from your website and use web forms instead.** Web-based contact forms are often safer for survivors to use because the communication happens within the website (instead of through the survivor’s email account where a sent message might later be found by the abusive partner). It is also important to include questions about the safety of reaching back out to them. See NNEDV's Contact Us form as an example.

5. **Use HTTPS**

   HTTPS means that an eavesdropper won’t be able to see which pages on your site were visited and, most importantly, won't be able to read any information submitted on your web forms. Configuring your website for SSL/HTTPS also has the added benefit of improving your rankings in search engines as well as giving your organization an increased sense of legitimacy.
NOTE: Even with HTTPS, an eavesdropper can still see that someone visited your site, just not the details of what they did there. And, if someone is using spyware or keystroke logging, HTTPS doesn't protect against that.

6. Add a link to NNEDV Safety Net Project's [Tech Safety plan](#). The safety plan is in eight languages. If you are in Canada, Europe, or elsewhere, ask Safety Net for a version that's adapted your country/province and post that to your website.

7. Get informed consent for names, photos, documents and videos that you post to your website and social media pages. This includes presenters, donors, boards, staff, volunteers and other individuals whose information you publish (including in emailed newsletters). Remove any content that your organization does not presently have explicit consent to post. In addition, remove geotags from photos posted to your website. 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 mobile device with the location or geotag feature on.

8. Make your website more accessible. Ensure all people can access to your website's safety information. Check that the font you use is large enough, has strong contrast, and that images on your website have alternative text descriptions (alt text). For links, use the format we’ve used in this handout: describe where the link is going and embed the link in that text. Read more at the Web Accessibility Initiative's [Tips for Getting Started with Web Accessibility](#).

© 2018 National Network to End Domestic Violence, Safety Net Project. Supported by US DOJ-OVW Grant #2016-TA-AX-K064. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ. We update our materials frequently. Please visit [TechSafety.org](#) for the latest version of this and other materials.