Appendix 8: Covering Your Tracks

If you are a victim of abuse, you may put yourself at risk if your abuser is able to "track" your computer use of the internet or email, if they identify the last telephone number you called, if they receive or access your voice mail or text messages, or if they can check your telephone bill for phone numbers called.

FOR SAFE COMPUTER USE:

- Do a Web search on "cover your tracks" or "cyberstalking".
- Check internet resources specific for victims of domestic violence and follow their instructions on internet and email safety, for example:
- Find and use a computer at a public library, an internet café, at the home of a trusted friend, a shelter for women, school, other community resources, or at work.
- Use an email password that your abuser will not know or be able to guess. Do not write down your password.

Browsers like Chrome, Internet Explorer, Firefox and Safari leave traces behind indicating where you've been and what you've been looking at on the Internet. Using 'Incognito' or similar mode can keep browsing private.

What things are included in my history?

Browsing & Download History: Browsing history is the list of sites you've visited that are shown in the History menu, the Library window's History list, and the Location bar autocomplete's address list. Download history is the list of files you've downloaded that are shown in the Downloads window.

Form & Search Bar History: Form history includes the items you've entered into web page forms for Form autocomplete. Search Bar history includes items you've entered into Firefox's Search bar.

Cookies: Cookies store information about websites you visit, such as site preferences or login status. This includes information and site preferences stored by plugins such as Adobe Flash. Cookies can also be used by third parties to track you across sites. For more info about tracking, see How do I turn on the Do Not Track feature?.
Note: In order to clear cookies set by Flash you must be using the latest version. See Updating Flash for instructions.

Cache: The cache stores temporary files, such as web pages and other online media, that Firefox downloaded from the Internet to speed up loading of pages and sites you've already seen.

Active Logins: If you have logged in to a website that uses HTTP authentication since you most recently opened Firefox, that site is considered "active". Clearing this logs you out of those sites.

Offline Website Data: If you've allowed it, a website can store files on your computer so that you can continue to use it when you are not connected to the Internet.

Site Preferences: Site-specific preferences, including the saved zoom level for sites, character encoding, and the permissions for sites (like pop-up blocker exceptions) described in the Page Info window.

HOW TO COVER YOUR TRACKS SURFING THE WEB

It may not be safe for you to access sites for information about family violence from your computer. Your abuser could discover what sites you have visited. To hide your internet activities you need to clear the computer's memory of the most recent pages you have accessed on the Internet. Here's how to reduce the chances that your net travels will be traced.

If you use Internet Explorer:

Pull down the Safety menu, select Delete Browsing History.
Select Temporary Internet Files, Cookies and History.
Click Delete.

If you use Microsoft Edge:

Open the menu by clicking the three points in the top right corner.
Go to the settings menu.
Under "Clear Browsing History" click the "Choose what to clear".
Select Temporary Internet Files, Cookies and History.
Click clear.

If you use Firefox:

Click on the three bars on the top right bar.
Open the history menu.
Use the clear recent history button.
Select the correct amount of time to clear.
Click clear now.

If you use Google Chrome:

Open the menu by clicking the three points in the top right corner.
Under the more tools menu open "Clear Browsing Data".
Select the desired amount of time to clear.
Make sure that "browsing history" and "cached images and files".
Click the clear browsing data button.

If you use Safari:

Pull down the Edit menu, select Empty Cache, and click Empty.
Pull down the History menu, select Clear History.

If you use AOL:

Pull down My AOL, select Preferences.
Click on the WWW icon under Temporary Internet Files, click on "Delete Files".
Under History, click on "Clear History".
If you do not know which browser you are using, pull down the Help menu, and click on About. Please note, certain browsers update regularly and may change the steps required to clear your browser history.

A cleared history may raise suspicion. Once you have cleared your history, it is a good idea to access some sites on other subjects after you have cleared the cache so that it will have some items in it. For instance, check out the sites of newspapers, government, or entertainment.

Bright Sky is a safe, easy to use app and website that provides practical support and information on how to respond to domestic abuse. It is for anyone experiencing domestic abuse, or who is worried about someone else. The app can be set to appear as a weather app, a game or a calendar app. Bright Sky is available for the App Store or Google Play.

FOR SAFE TELEPHONE USE:

Change your access code for phone messages if your abuser knows the code used. Do not write down your access code.

Find and use a public telephone or use a secure telephone at work or of a trusted friend.

Have a trusted friend or co-worker receive telephone messages for you (for example, if you are receiving calls from a lawyer, local shelter, police, etc.)

When people are leaving you voice or text messages, ask them to be careful and to not identify the nature of the call or service.

Seek permission to use workplace resources – such as computers or telephones – to find information, so long as these resources are not available to your abuser.

Co-workers, managers, union representatives or others in the workplace might be willing to receive messages on your behalf or help you to find resources.