Internet Safety

Warning: Following the actions on this page may **NOT BE ENOUGH** to prevent an abuser from tracking your online activity and ensuring your safety. The safest way to find information online is to use a computer at a library, a friend's house, or work. If you have further questions or would like to better understand your technology options, please contact the National Domestic Violence Hotline: 1-800-799-7233.

Communication Safety Overview

Communication via telephone or Internet is not necessarily confidential. You may be leaving behind information that can give your abuser clues about who you are contacting or what types of information you are searching for when you browse the Web, send email or instant messages, or use your telephone. There are many tricks for decreasing your risk, but it is very difficult to clear or hide all the information that is left behind.

How to Ensure Private Communications

The information below can assist you in protecting the confidentiality of your communications. It is not an exhaustive list of preventative measures, and it does not guarantee the safety of your communications.

Because an abuser could install monitoring software that secretly records the programs you run, the files you access, and what you type, the best way to ensure private communications is to use tools that your abuser is not able to access. Examples include:

- Computer at your workplace
- Computer at a public library
- Computer at your local domestic violence shelter
- Pay phone
- Friend's cell phone
- Cell phone obtained from a domestic violence program

Email Tips

Email Account Access

If an abuser can access your email account, he or she will be able to read any sent or received email that you have not deleted. You should consider having more than one email account, so that you have an alternative if your abuser gains access to your account or forces you to terminate your account.

Web-Based Email Programs

Use a Web-based email service for correspondence that you wish to remain private. There are many free services such as Gmail and Yahoo! Mail. These Web-based email

services can be used from any computer that has Internet access, and they will not store information on that computer. Web-based email accounts are safer than utilizing local programs such as Outlook Express, Eudora, or Thunderbird that store sent and received emails on your computer.

Web-Based Email Account Set Up

When setting up your Web-based email account:

- Do not use identifiable information in your e-mail address.
- Ask your close friends and family to not share your new address.
- Don't select a username that includes your name.
- Don't register personal information such as your real address or phone number when you sign up.

If You Use a Local Email Program

If you do use a local email program, there are a number of ways to minimize your risk:

- Choose a password that would be difficult for anyone else to guess.
- Do not share your password with anyone.
- When you send email that you wish to remain private, delete it from the Sent folder and delete it from your Trash folder or Deleted Items folder.
- Save threatening or harassing emails that you have received from an abuser as evidence of abuse. You may also wish to print these messages and either give them to a friend or hide them in a secure location.
- Do not check any defaults that allow the computer to remember information. Examples include "Remember my Username" or "Remember my Password."

Web-Browsing Tips

It is very difficult to completely cover your tracks when browsing the Web. Many traces of information about your activities on the Internet are stored on your computer. The best option is to use a safer computer as suggested above under How to Ensure Private Communications.

Clear History/Cache

If an abuser knows how to read the history or cache (automatically saved Web pages and graphics) from your Web browser, he will be able to view recent sites that you have visited on the Internet.

To maintain your privacy, you should clear your history and empty your browser cache after every session of Web browsing. The method for doing so varies depending on your browser and version. Several popular browsers are listed below. If your browser is not

listed, find the Help menu in your browser and search for “cache” and “history” for information on clearing these items.

Microsoft Internet Explorer

To clear your browsing history in Internet Explorer, select Tools, then Delete Browsing History. Click the button for Delete All. Select the check box for Also delete files and settings stored by add-ons and click Yes.

Mozilla Firefox

To clear your browsing history in Mozilla Firefox, select Tools, then Clear Private Data or Clear Recent History.

Alternatively, you can set a default preference that will automatically clear private data when you close the Firefox browser. On a Mac, select Firefox, then Preferences. Under the privacy tab, select the check box for Always clear my private data when I close Firefox under the Private Data subhead. On a Windows machine, select Tools, then Options. Under the privacy tab, select the check box for Always clear my private data when I close Firefox under the Private Data subhead.

Altering Your History and Cache Habits

Be careful when altering your Internet-use habits. If you are being monitored by your abuser, suddenly deleting your history and clearing your cache may arouse suspicion and put you in danger. Either switch to a safer computer as suggested under How to Ensure Private Communications, or refill your history list by visiting other sites that you visit frequently before exiting your browser.

Additionally, if you do switch to a safer computer, you may want to continue to use the monitored computer for normal browsing so as to not arouse suspicion. Use the safer computer for seeking assistance, job hunting, apartment seeking or researching an escape plan.

Forums, Newsgroups, and Social Networking Sites

To protect yourself when posting to forums, newsgroups, or social networking sites, you should not use recognizable personal information in your screen name or postings such as:

- Your name, location, or pet’s name
- Your city or town
- Places (concerts, events, museums, shows) that you have visited

Passwords

Selecting a strong password and keeping it secure is one of the best ways to protect your information. Some password tips include:

- Do not automatically store passwords or add passwords to the Keychain on a Mac. This makes it very easy for an abuser to access your accounts.
- Select passwords that are difficult to guess. Do not use your name, birthdate, street address, or pet's names in your password.
- Use passwords that include a mix of numbers, letters, and other characters (!, #, *) to make them more difficult to guess. Use at least six characters.
- Change your password frequently.
- Do not write down your passwords.

File Storage

If you have sensitive digital files that you wish to remain confidential, consider storing them online. Services such as Google Docs, iBackup, Xdrive, and box, allow you to store files on the Internet and access them from any computer.

Telephone

It's easy to forget that your telephone may not be private. The following tips can help protect your privacy:

- Traditional corded phones are less prone to interception than cordless phones or cell phones.
- Be aware that cell phones have Global Positioning Systems (GPS) location tracking features that an abuser could use to find out where you have been.
- Contact One Place or Hopeline for information about free cell phone donation programs.