COVERING YOUR INTERNET TRACKS

COVER YOUR TRACKS

Your internet, e-mail and document use activities leave traces on your computer that can be found. Use a computer to which those you are fearful of do not have access to, such as at work, in a library, or a friend's computer. If you do use your own computer, complete the following steps to provide some measure of protection for you and to remove most traces of your computer activities. Be advised, however, that these steps will not remove all traces of your computer activities.

Using a "Live CD," however, will ensure that you leave no traces. You can find one at one from www.ubuntu.com by downloading and burning the CD for yourself. You can get one free in the post by going to www.shipit.ubuntu.com. Once you have your Live CD, start the computer with it in your CD drive allowing it to boot the computer from the CD drive and giving you the opportunity to run the Ubuntu Linux Operating System directly from the CD. No traces will be left on the machine unless you specifically allow it.

DO NOT STORE

Do not use obvious passwords, such as your birthday or your pet's name. Use passwords that include both letters and numbers. If you are concerned about forgetting your passwords try "KeePass" Password Safe where you can store all your passwords in one place protected by the one password you must never forget. If you do forget it there is no way to get your information again. You can store KeePass on a USB flash drive but keep a backup elsewhere in case it is lost.

DELETE E-MAILS

Delete e-mails from the "Send" or "Outbox" and then also delete e-mails from the "Deleted Items" box. In addition, empty the "Recycle" or "Trash Bin" of any documents before shutting down the computer. Make this a regular routine so it is not an unusual action that may trigger suspicion. You can also use software that permanently removes all trace of your sensitive files.

CLEAR SEARCH ENGINE

Search engines can retain and display past searches. With AOL, searches can be cleared on the Web Matches pages. In Google, Hit the "Clear All" icon under Recent Search History. The listing of recent searches can be disabled by hitting the "Turn Off" icon under "Recent Search History." Other search engines may also retain and display searches. Check any search engine that you use for this function. A good exception to this is www.scroogle.org/cgi-bin/scraper.htm which takes the useful information from Google and discards search history.

CLEAR COOKIES, TEMPORARY WEBSITE FILES AND BROWSER HISTORY

Cookies are information that a website leaves on your hard drive about your visit to that website. A temporary website file is left on your computer each time you visit a website. One of its pages, usually the home page, is stored temporarily on your hard drive. Usually internet browser software retains a list, or history, of all the websites you visit. To clear cookies, temporary website files and history for browsers, click the "Tools" menu on your Internet Explorer browser. Select "Internet Options." In the "General" tab, and under the "Temporary Internet Files" section, click "Delete Temporary Internet Files". Click OK to close "Internet Options." Close all your browser windows and restart your browser. You can refer to your software "Help" menu or technical support for further information with regards other browsers.

PORTABLE APPLICATIONS

Portable applications are a good way to use a "Windows" computer without leaving information on the hard drive unless you choose to. They can be run directly from any external hard drive such as a USB flash drive, PDA, some mobile phones, SD card, some MP3 Players, etc. You can get a safe Portable Application from John T Haller's Portable Apps (applications - programs) at www.portableapps.com. Ideally get Firefox Portable from www.portableapps.com/apps/internet/firefox_portable first so you can continue surfing using Firefox without leaving further traces on the computer. When you run the file you downloaded it will start an install wizard which asks where you want to install so use the "Browse" button to navigate to your USB flash drive. Once it is installed there will be no entry in the start menu or shortcut on the desktop so you must run it directly from the USB flash drive. Be patient, it may run slower from USB than from hard disk. Now you can head back to http://portableapps.com/apps and more useful things like KeePass Password Safe Portable - Secure, easy-to-use password manager, Eraser Portable - securely delete files and data (shredder) and EraserDrop Portable - easily secure-erase files and data.

KEEP UPDATED

In computing, there are always alternative ways of doing things and what works well today may change tomorrow. For more tips and updates on staying safe search the internet for terms like safety, privacy, Firefox, "Live CD", cookie, USB, etc.