

Covering Your Tracks: How to Keep an Abuser from Viewing Your Internet Activity

Note: Since computer programs are constantly changing and several different types of programs are available this information does not cover all aspects of covering your tracks.

Computer use such as e-mail and Internet use can provide quick access to important information for sexual assault survivors. However, if you are concerned an offender may be tracking your computer activities, here are some safety tips to try to maintain your privacy and increase your safety. There are also computer programs available to do all of this for you.

Warning: If the abuser is computer savvy, you may not want to follow some of these procedures. He/She may notice changes have been made.

Terminology used in this article:¹

Administrator: Person in charge of maintaining the computer. Some of their tasks include adding/deleting users, security, and monitoring the system performance. Computers running the Windows Operating system come with the account "Administrator" already created. See your computer manual for initial password information.

Browser: A computer program used to view web pages (e.g., Mozilla, Netscape, Internet Explorer, AOL)

Cache: An area of your hard drive that stores the web pages you viewed. This allows for the pages to be loaded quicker if you decide to view them again.

Cookie: A small text file that is saved on your computer, which allows websites to save your preferences.

E-mail: Electronic mail. Mail sent over the Internet.

Internet: Developed in the early 1960's by the Advanced Research Projects Agency (ARPA, now known as DARPA) for the United States Department of Defense as a means of connecting nuclear weapon arsenals. Today, the Internet consists of computers connected from all over the world.

History: A list of web pages you have recently viewed. These are easily accessible by clicking the Forward or Back button in your browser.

Passwords DOs and Don'ts:

- **Do** change your password as often as you feel necessary to keep safe.
- **Do** keep your password and login information to yourself.
- **Do** choose a password that includes a combination of letters or numbers. This makes it more difficult to determine.
- **Do NOT** share your login and password information with anyone else. Create a User account for each person that uses the computer. Follow the steps provided in your computer manual.
- **Do NOT** assume that because you kept your information to yourself that someone cannot log into your account. Anyone that knows how to gain administrative rights to your computer can easily find out your login and password information. Check your user's manual to see what the initial administrator password is. This password should be changed to prevent others from logging into your system. Be sure to remember it or else you will not be able to make changes to your system in the future.
- **Do NOT** write down your password ANYWHERE. No sticky notes on the computer screen or slips of paper in a drawer or purse.
- **Do NOT** assume people cannot get through your password defense. You need to take precautions to cover your e-mail and browsing trail.
- **Do NOT** choose a password that is easy to guess. No pet's names, children's names, etc...



E-mail:

- Keeping your e-mail on your computer makes it easy for someone to read all about your life and activities.
- Set up a browser based e-mail account such as www.hotmail.com. **DO NOT** choose an e-mail provider that requires you to enter your dial up e-mail address! They will send sign up information to that e-mail address and if you are not there to get it, someone else will. Since these e-mail accounts allow you to store your messages on THEIR machine, set up some folders in your mail account and save your messages online.
- Make sure you send all your outgoing e-mail using one of these browser based mail accounts. If the settings are not correct on some mail programs, you could be leaving a trail on your computer.
- Remember to save and print all e-mail from a stalker/abuser. This could be used as evidence. If it is not safe for you to print them out or save them safely on your computer, forward them to your online mail account and store them there.
- If you decide to use an e-mail account on your computer (e.g., Outlook, Netscape Composer) change the preference/options to NOT save your sent messages. (Do save a copy of messages sent to abuser as evidence.)
- Remember to empty the “Deleted” folder.

Browsers:

Your browser (e.g., Netscape, Internet Explorer, AOL) keeps a lot of information about you. Before you walk away from your computer always clear cache, clear history, clear cookies, and **CLOSE THE BROWSER** (terminate the browser program). Also remember if you bookmark a site (also known as “Favorites”) other people can easily use your bookmarks to see where you have been.

Clearing the Cache/History: These items are typically found under one of the pull down menus at the top of the browser. They are usually found under the labels “Options” or “Preferences” and the terminology varies slightly for each browser.

Clear Cookies: Cookies help websites keep track of your information on their website. Cookies are commonly used for account login and shopping. When you are done using your browser “Remove All Cookies” if the option is available.

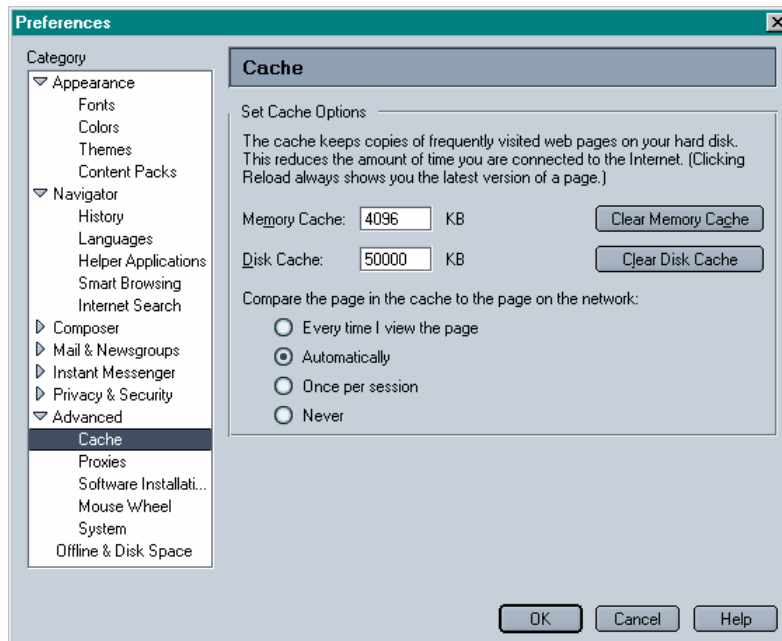
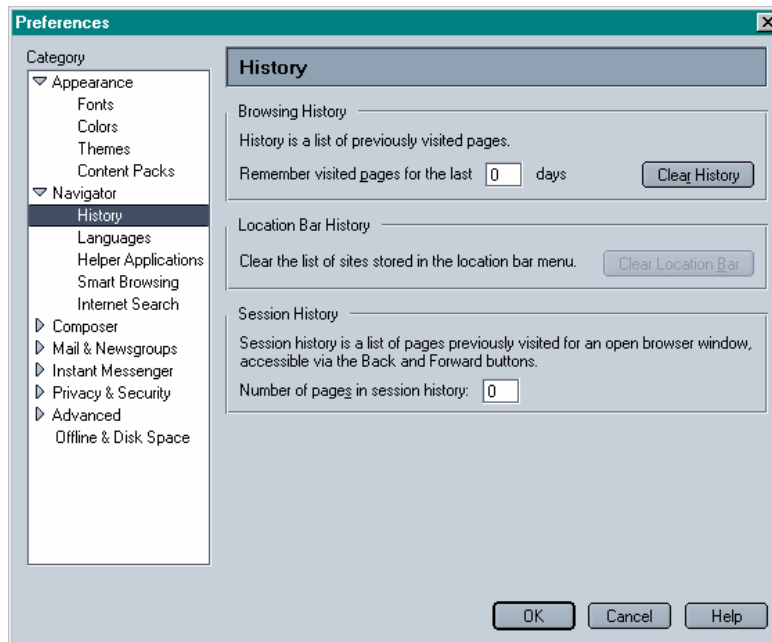
Disable “AutoComplete”: Auto complete remembers what you typed into a form and stores the information to assist you in completing future forms.

Empty “Recycle Bin”: When you have completed all the above tasks, empty the “Recycle Bin”, because it will contain many of the files you just deleted.

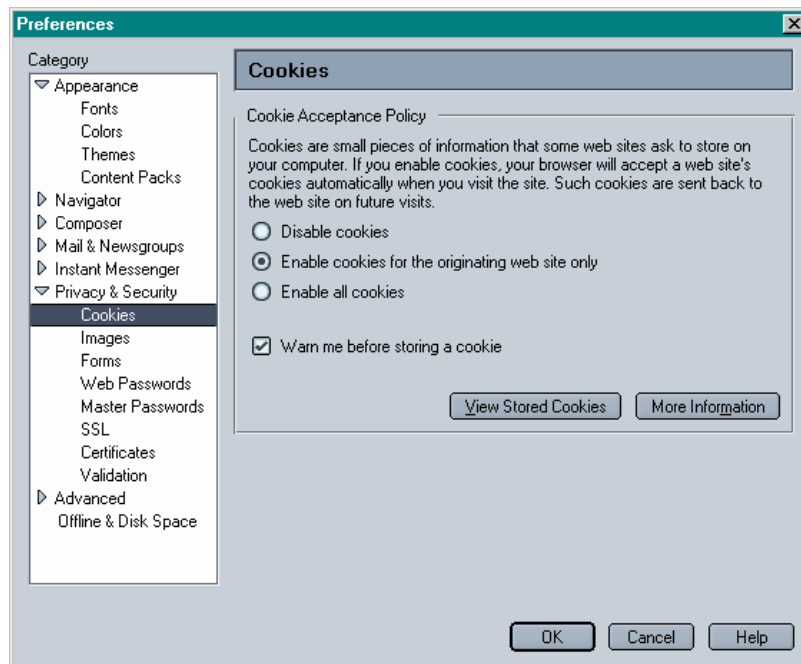


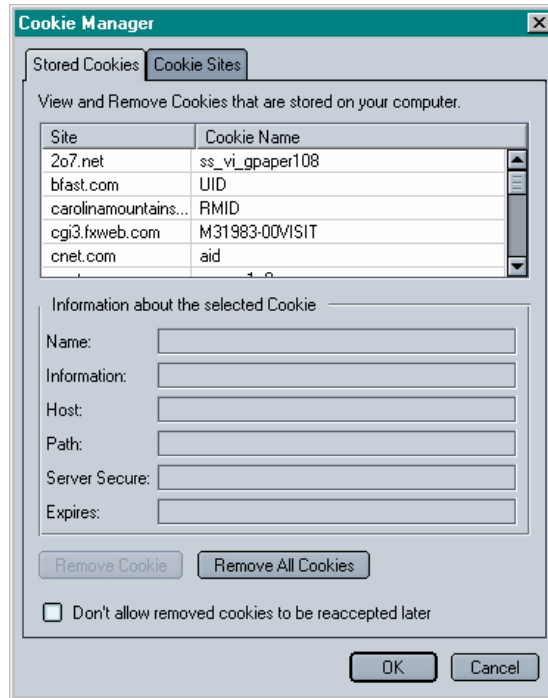
Netscape 6.21

- Under “History” set “remember visited pages for the last” to “0” days and click “Clear History”
- Change “Number of pages in session history” to “0”
- Under “Advanced” > “Cache” click “Clear Memory Cache” and “Clear Disk Cache”
- Click “OK”



- “Under Privacy & Security” > “Cookies” Click “View Stored Cookies”
- A new box will open. Click “Remove All Cookies”



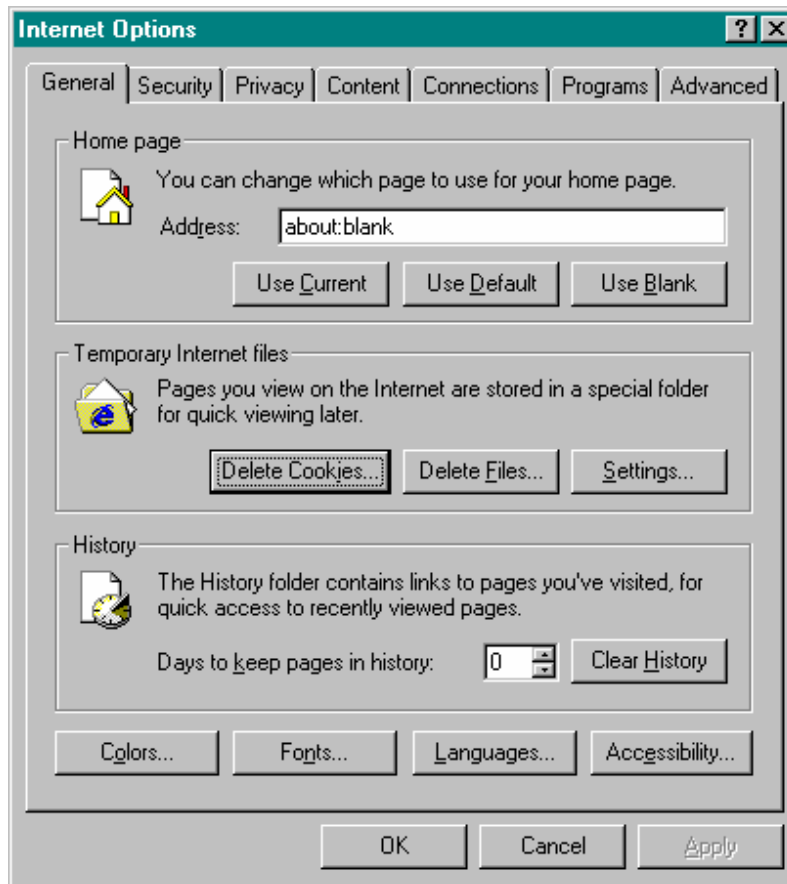


Internet Explorer 6.026

Under the "General" Tab

- Click "Delete Cookies"
- Click "Delete Files"
- Set "Days to keep pages in history" to "0"
- Click "Clear History"





Under the “Content” tab

- Click “AutoComplete”: a new box will pop up
- Uncheck “web addresses, “forms”, and “user names and passwords on forms”
- Click “Clear Forms”
- Click “Clear Passwords”
- Click “OK”





Reference:

¹The Internet, 2nd Edition, Perry, Kames T., Schneider, Gary R., Course Technology 2000

