If you are dealing with a partner or ex-partner who at any time has:

- monitored your phone calls
- stopped you from visiting with your friends or family
- had his family and friends keep tabs on you
- become extremely jealous when you've seemed interested in other people
- limited your access to the car and/or tracked the car mileage
- controlled the family money
- threatened your safety and/or the safety of the kids
- hurt or threatened to hurt your pet
- physically hurt you and/or the kids

or if you are being stalked or experiencing harassment in a workplace in which computers are often used, you need to read the following information very carefully.

The Internet can be a great place to get information and to make or maintain friendships. However, your activities on the Internet can be tracked quite easily. If someone wants to control you or wants to find out what you are doing, there are many ways they can gather this information.

There are also ways you can protect yourself as you use the Internet. The following suggestions can help you cover your tracks as you surf the web, use chats or send email. However, remember that NONE of these can protect you COMPLETELY.

Use a Safe(r) Computer

When you surf the web or send email, use a computer your abuser or his friends, colleagues and family or even your kids will not have access to.

Local libraries, community centres and some women's shelters and rape crisis centers have computers available for free public use of the Internet. Or use a friend's computer or, if possible, one at work (unless this is where you are experiencing abuse and harassment). If you have no choice but to use your abuser's computer, a computer you share, or a computer that he has set up for you, see below for some ways to Cover Your Tracks.

After using a computer in a public place, be sure to clear your Internet history (see Cover Your Tracks: Visiting Websites below) to give yourself a little privacy. Be aware that unless the computer terminal is in a secluded location, others may see what appears on the computer screen.

Exercise Email Caution

A note about email: There are two ways to access email. One is through a "web-based" email program. This means you check your email through a website and need a password every time you open your email. There are free options for web-email: Hotmail.com and Yahoo.com are two examples. The other way to access email is through a program that's located on your computer. This will require a password only to open email, not to send it. MicroSoft Outlook and Eudora are examples. If you are living with an abuser and can keep your password secret, it's safer to use a web-based email program.

Never send email containing confidential information or information that may threaten your safety if your abuser reads it.

Emails sent through programs that are not web-based get stored in your computer. There are ways you
can delete them off your computer (see "cover your tracks" below) but an abuser can install software that will record everything you type (your "keystrokes") so even web-based email is not safe. Even if you are using a computer that your abuser has no access to, emails are stored by your "service provider" or "ISP" (the service that connects your computer to the Internet) or by the email service (Hotmail or Yahoo). This information can be subpoenaed by lawyers or police.

Emails can also be accidently sent to the wrong person, redirected (your receiver can send them on to someone else), or copied. Sometimes emails will simply not reach their destination, due to technical problems.

**Take care with passwords.** If you share a computer with your abuser or he may have access to it, always chose a password for your email account that he will not be able to guess (this may be the only time he remembers your date of birth). Email programs that are set up on your computer (as opposed to web-based email like Hotmail or Yahoo), do not require a password when a person sends out an email. Your abuser may use this technical flaw to collect information about you from unsuspecting friends or relatives or other advocates that you have sent email to. He may send email to these people and pretend that he is you and ask recipients to send the response to another email address.

**Using the Web for Help.** If you consider contacting an organization for help through email, find out what their policies are on maintaining your confidentiality. Read the OWJN Disclaimer for the policy on the emails OWJN receives. Please tell us, or any organization you contact, if you feel that your Internet activities may be monitored by your abuser. It may be safer to phone an organization rather than send an email.

The **Assaulted Women's Helpline** can be called toll-free from anywhere in Ontario at **1-866-863-7868** or **TTY 1-866-863-0511**. website: www.awhl.org

For more information on email safety, visit the cyberstalking page on the METRAC site, at [http://www.metrac.org/programs/info/cyber.htm](http://www.metrac.org/programs/info/cyber.htm).

**Cover Your Tracks**

There are ways to remove some evidence of your activities on the Internet. However, an abuser who is determined can trace your movements pretty easily even if you follow all the instructions below. It does not take any special computer expertise to follow another person's activities. PLEASE be cautious if you share your computer with your abuser.

**Email**

1. If you don't want a record of it, don't say it in an email.

2. Avoid using email programs that are on your computer. Sign up for a free email account through a web-based service instead. Ask a friend to provide the contact information this service will require before they issue you an account. You will be able to access this account from any computer that is hooked up to the Internet. Protect your password. Be aware that with some expertise, these accounts can be traced. (If you are being stalked, stay clear of this sort of email.)

3. If you must or already have **sent** an email that may endanger you from a computer you share with your abuser,

   - delete the email from the "Out" or "Send" box of your email program then delete it from the
“Deleted Items” or “Trash”
If you have received an email that would endanger you if your abuser saw it, delete the email from your "In" or "Received" box then delete it from the “Deleted Items” or "Trash"

However, keep in mind 1) that someone with technical skills can recover this information from the hard drive of your computer, 2) that certain software installed on your computer can document everything you type, 3) that another copy of the email is saved on your service provider, and 4) that a copy exists with the receiver or sender of the message.

**Chats (IRC), Newsgroups, Mailing Lists, Bulletin Boards, etc.**

Anything you post to an online discussion forum is probably archived and will be available to the public through Internet searches. As with email, don't say it if you don't want a record of it.

Some chats have an "enable/disable log" setting; select "disable" to prevent a log from being kept. However, remember that your abuser may have installed software on your computer that can record everything you type. Or, if an abuser suspects your use of a particular chat, mailing list, etc., he may join and "lurk" or participate in a disguised identity.

**Visiting Websites**

A "browser" is a computer program that helps you see websites. Most people use the Internet Explorer browser although some use Netscape Navigator/Communicator and others.

When you surf the web, your browser maintains a record of the websites you visit. If your abuser has access to your computer, he can track your movements by looking at these records. Information on where you go on the web is recorded in the Location Bar, History and Temporary Internet Files or Cache of your browser. To cover your tracks, you will want to delete parts or all of the information in these locations.

Before you make any changes, have only one browser window open. (You may wish to close and reopen the browser program.) **After you make the changes, close and restart the browser.**

Steps for changing browsers vary. To learn the specifics of your browser, you need to know the name of the program and the version number, which will appear briefly on your screen when you start up the program. You can enter this information into a search engine with terms such as "clear cache" or "clear location bar". Alternatively visit this Yahoo! Help page: [http://help.yahoo.com/help/us/mail/errors/errors-17.html](http://help.yahoo.com/help/us/mail/errors/errors-17.html) for information on clearing your cache for various versions of Netscape and Internet Explorer.

An abuser may become suspicious of an empty History or Location Bar or Cache. Erasing all the information from these locations will also erase all the sites your abuser has visited and he may wonder why they are no longer in the browser's memory. Therefore, you may want to try deleting only select items. Some examples for how to do this follow.

**Browser: MicroSoft Internet Explorer 5 for Windows**

To clear your cache:

- Select "TOOLS" from the bar of buttons at the top of your screen,
  - then choose "INTERNET OPTIONS",
  - select the "GENERAL" tab in the top left corner of the screen.
• In the middle of the box where it says "Temporary Internet files", click on "DELETE FILES."

To clear your **entire** history:

• Select "TOOLS" from the bar of buttons at the top of your screen,
• then choose "INTERNET OPTIONS",
• select the "GENERAL" tab.
• At the bottom of the box that appears on your screen, click on "CLEAR HISTORY."

To clear **only specific websites** from your history:

• Go to a website that you do not need to remove from your browser history.
• Then click on "FILE" in the top left corner of the bar at the top of the screen
• chose "WORK OFFLINE".
• Next, select "HISTORY" from the buttons near the top of your screen (it will be near "FAVORITES").
• A side bar will appear on your screen listing all the sites you have visited.
• Highlight the site you wish to remove;
• a box will appear;
• select "STAY OFFLINE".
• Delete the site.

**Browser: Netscape Communicator for Windows**

To clear your **entire** history:

• Go to "EDIT" in the bar of buttons at the top of your screen,
• then choose "PREFERENCES".
• Click on "CLEAR HISTORY" in the box that appears on the screen.
• You will then have to clear your Location Bar (the bar that contains the address of the site you are presently visiting) by selecting the EDIT button,
• then PREFERENCES and clicking on "CLEAR LOCATION BAR".

To clear **only specific websites** from your history:

• Go to go to "COMMUNICATOR" in the bar of buttons at the top of your screen,
• select "TOOLS" then "HISTORY".
• Highlight the individual items you wish to delete.
• You will then have to clear your Location Bar (the bar that contains the address of the site you are presently visiting) by selecting the EDIT button,
• then PREFERENCES and clicking on "CLEAR LOCATION BAR".

To clear your **cache**:

• Go to “EDIT” in the bar of buttons at the top of your screen,
• then choose “PREFERENCES”.
• On the left hand side of screen, click on the "+" in front of "ADVANCED",
• then select "CACHE".
• Select "CLEAR MEMORY CACHE" and click "OK".
• Select "CLEAR DISK CACHE" and click "OK".
• Click "OK" at the bottom of the screen.

If you are working on a computer to which your abuser has limited or no access, you may wish to change the number of days your browser records sites to zero. Do so by selecting the number that appears beside the "CLEAR HISTORY" buttons. An abuser who shares your computer may become suspicious if this number has been changed.

After you have deleted dangerous sites from these locations, you may want to add a few so that it is not obvious you have removed information. Visit your children's favorite t.v. shows, recipes sites, weather sites or other topics that won't arouse your abuser's interest.

**Cookies**

Another item on your computer's hard drive that will provide some record of your activities on the web are "cookies". Cookies are mini-tracking programs that many websites attach to anyone who visits. A cookie is placed on your computer hard drive and allows the sending website to track your activities as you visit their site.

A cookie on your computer can almost always be traced back to the website that first placed it. In fact, software exists that lets another computer check your computer's cookies. This means that an abuser can check the cookies on your computer even if he does not have *physical* access to your computer.

Most sites that provide safety information for women who are dealing with violence do not use cookies because they can endanger their users if abusers find the cookies and trace them. However, sometimes cookies ARE used. Therefore it's important to disable your cookies while you surf, even though this can be annoying.

**To disable your cookies:**

**Browser: MicroSoft Internet Explorer 5 for Windows**

• Select "TOOLS" from the bar of buttons at the top of your screen,
• then choose "INTERNET OPTIONS",
• select the "SECURITY" tab.
• You need to customize this section, so click on the button "CUSTOM"
• scroll down the list to "COOKIES".
• You will need to "DISABLE" them and then click on "RESET" to establish these changes in your browser's settings.

**Browser: Netscape Communicator for Windows**

• Select the EDIT button in the top left hand corner of your screen,
• then choose PREFERENCES
• click on "ADVANCED" under "CATEGORY".
• In the COOKIES box, select "DO NOT ACCEPT COOKIES".

**Cyberstalking/Online Harassment**

Cyberstalking is a term used to describe harassing behaviour that happens through email,
newsgroups, chats and websites. Often cyberstalking is just another form of harassment an abuser performs: a guy a young woman won't date appears in her favorite chat; an aggressive co-worker sends increasingly threatening emails; or an emotionally abusive man posts embarrassing pictures of his partner on a website.

One of the most important things to remember about cyberstalking -- as with other forms of harassment -- is to collect evidence of the harassment even if you have not yet considered going to the police. Save email, mailing list correspondence, and chat logs. Save the links and download the source code of harassing websites (in Explorer, go to "VIEW" and then click on "SOURCE"; in Netscape, go to "VIEW" then click on "PAGE SOURCE"). Put this information on disks and keep the disks in a secure place. Although you may feel that keeping anything associated with your harasser/abuser as abhorrent, if the harassment escalates, you can give this evidence to the police.

For more information on cyberstalking and links to organizations that can help, visit the METRAC website at: http://www.metrac.org/programs/info/cyber.htm.

Emergency Resources

If you feel you are in danger because an abuser may be monitoring your computer activities or harassing you online, we urge you to contact your local women's organization (their phone number will be in the front of the phone book) or call the province-wide service, the Assaulted Women's Helpline at 1-66-863-7868 or TTY 1-866-863-0511. If you believe you are in immediate danger, PLEASE call the police or 911. Take care!

Other Sites with Information on Covering Your Tracks

http://www.rosenet-ca.org/history.htm
"Protect Yourself" from Rosenet: Canadian Law and Abused Immigrant Women - includes screen images of clearing your history and temporary files

http://www.jewishwomen.org/Warning_Erase.htm
"How an Abuser can Discover Your Computer and Internet Activities" on the Jewish Women International site

"Hiding Your Tracks On-line", the Domestic Violence site of the City of Fremantle, Australia

http://www.kcsdv.org/plan.html#websafety
"World Wide Web Safety" page of the Kansas Coalition Against Sexual and Domestic Violence site

http://www.shepherd.edu/compserv/prevent/internetch.htm
This page of the Shepherd College (West Virginia) website provides pictures of the step-by-step cleaning up of caches and histories on both Internet Explorer and Netscape: "Cleaning up the mess Netscape and Internet Explorer make on your hard drive"

http://www.haltabuse.org/
WHOA – Working to Halt Online Abuse: an excellent resource for any one who is being harassed while online. American.

http://www.metrac.org/programs/info/cyber.htm
Information on cyberstalking, including ways to protect yourself and resources, on the METRAC
website.

http://www.womenspace.ca/equality/tools/privacy.html
Tools for safety and privacy on the internet from Womenspace.

http://www.metrac.org/programs/info/assess.htm
Tips on assessing websites from METRAC.

http://www.serve.com/zone/
Safety Zone, one of the first sites to recognize the potential dangers of the Internet to women who are experiencing violence.