

# Cyberstalking

Prepared by the Canadian Resource Centre for Victims of Crime

The Internet has become a widely used tool of communication. Millions of people around the world have access to the Internet and the wealth of information it provides. A recent phenomenon called cyberstalking has been gaining global attention. Cyberstalking can be defined as threatening behaviour or unwanted advances directed at another using the Internet and other forms of online communications.

The vast amount of information and limitless boundaries make policing the Internet an ominous task. Without tangible laws to govern its use, sexual predators and stalkers have free reign. Cyberstalkers target their victims through chat rooms, message boards, discussion forums and e-mail. Cyberstalking takes many forms such as: threatening or obscene e-mail; spamming (in which a stalker sends a victim a multitude of junk e-mail); live chat harassment called flaming; leaving improper messages on message boards or in guest books; sending electronic viruses; sending unsolicited e-mail; and electronic identity theft.

Cyberstalking usually occurs with women, who are stalked by men, or children who are stalked by adult predators. The cyberstalking victim is usually inexperienced online.

Cyberstalkers lurk in chat rooms just as pedophiles lurk near schoolyards. Be cautious and remember these important safety tips when using the Internet [as recommended by Cyberangels; an Internet safety specialist ([www.cyberangels.org](http://www.cyberangels.org))]:

## **IF YOU HAVE BECOME A VICTIM OF CYBERSTALKING:**

- Where the offender is known, send the stalker a written message indicating that any further contact is unwanted.
- Victims should not communicate with the stalker after the warning message.
- If harassment continues, the victim should contact the stalker's Internet service provider, as well as their own.
- Service providers often have services to block and filter unwanted communications.
- Collect all evidence including e-mails, postings, or other communications in hard-copy or electronic form.
- Contact local law enforcement agencies to see what action can be taken.
- Consult your local computer store about encryption and privacy protection software.
- Consider changing your e-mail address, Internet service provider and home telephone number.
- Contact online directories to remove yourself from their listings.
- Never agree to meet with a cyberstalker to work things out face-to-face.
- Never leave your computer logged in unattended.
- Choose a good account password and change it frequently, the best passwords don't spell anything and don't follow a logical pattern.
- Make your password 7 letters long because the longer the password the harder it will be to break (there are more 7 letter words in the English language than 6 or 8 letter words).

- Review your e-mail signature and headers, do not reveal any personal information about yourself.
- Contact the International Web Police at [www.web-police.org](http://www.web-police.org), they fight crime on the Internet.
- Tell family, friends and co-workers about the harassment so that they can provide support.

For more information about Cyberstalking, please visit the following web site:  
<http://www.safetyed.org/help/stalking.html>

*Disclaimer: The information provided on this web site is intended for educational purposes only. Before implementing any intervention, please contact your local police service or Crown Attorney's Office for further and more specific information.*