Protection from Cyberstalking: Basic Advice

Social media is creating a world that is more open and connected, enabling people to share the most important parts of their lives with families, friends and communities. However, there are dangers online and technology can be misused by abusers and stalkers to spam, troll and harass you. Generally, most people don't think about cyberstalking until they are being harassed. You can control your safety and privacy online and deserve to be able to interact online without fear.

Listed below are some basic steps that individuals can take, at any time, to minimize their risk of being cyberstalked or to reduce the likelihood that the harassing behaviour continues.

Preventative measures* one can take:

- Choose a genderless screen name, and change it if necessary;
- Create a separate email account through a free service that is not tied to personal or work addresses, and is only used for online activity;
- Don't use your real name *or* nickname;
- Choose a complicated 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 passwords, the harder it will be to break (there are more 7 letter words in the English language than 6 or 8 letter words).
- Protect your privacy by not publishing or talking about your real name, address, or other contact details. Set privacy options to the most restrictive possible.
- Depending on level of threat, do not confront the aggressor. If the threat level is low, send a clear message that communication is unwanted. This will act as a benchmark for any future police investigations/legal proceedings. Once it has been sent, do not respond to any further communications.
- Never agree to meet with a Cyberstalker to work things out face-to-face.
- Never leave your computer logged in unattended.
- Use filters to remove unwanted communications, and block the user from interacting with you if possible (how to do this will vary by device or platform).
- Change passwords for all online points of contact, including email, IM, and social networks. If there is a risk that personal devices have been compromised, these changes should be made at a neutral site, such as a library.
- Don't have personal conversations in publicly viewable forums.
- Refrain from publicizing any plans (personal, vacation, travel, etc.).

- Learn cyber etiquette (lingo, profile rules, etc.) particular to the site being accessed.
- You can Google yourself to ensure no information is posted about you.
- If a situation becomes hostile log off and surf elsewhere.
- Keep a handwritten log of contacts from the cyberstalker, especially if there is a possibility that the computer/device has been compromised.
- DO NOT delete original messages. Save all harassing/unwanted messages, in soft and hard copy, this will be useful if reporting to authorities.
- Take screenshots of any harassing behaviours, especially those that are hard to log like video chats (how to do this will vary by device, use manual or internet search for instructions).

If You Have Become A Victim Of Cyberstalking:

- Contact local law enforcement agencies to see what action can be taken.
- Consider changing your e-mail address, Internet service provider and home telephone number.
- Contact online directories to remove yourself from their listings.
- Tell family, friends and co-workers about the harassment so that they can provide support.

For more persistent harassment or escalating stalking behaviours or threats, or if the cyberstalking moves from the online world to direct, in person contact, report it to the police immediately.

The National Network to End Domestic Violence (U.S.) and Facebook have teamed up to offer tips for survivors of abuse to maintain safety and control over their information: http://www.victimsofcrime.org/docs/src/nnedv-privacy-and-safety-on-fb.pdf?sfvrsn=4

***These suggestions assume that there is no imminent danger of physical harm. If there is such a threat, the victim must attend to their personal safety, by contacting the police, with the addition of family, friends and other appropriate supports.**

The following are more formal steps that should be taken if personal measures are not sufficient, if the stalking behaviours escalate, if the level of fear or threat increases, or the cyberstalking moves from the online world to direct, in person contact. While you would generally take these steps in the order listed below, their level of fear and need may necessitate taking several courses of action at the same time. **If there is imminent danger of physical harm, contact the police immediately by calling 911. It is a good idea to also advise family, friends and other appropriate supports about what is happening to you.**

Report the offender to your Internet Service Provider

The ISP is able to take action or propose measures that will discourage the harasser from trying to contact you. These steps may include directions on how you can change passwords/clean your system of any malicious software, or may extend to more advanced steps like blocking the user's IP address from contacting you. The offender will also be flagged in their abuse and security department. This may not resolve the problems, as staff is typically computer and network specialist with training in the resolution of technical issues - not victim support. Many ISPs do not inform their customers about what steps (if any) have been taken to follow up on the complaint and staff are constrained by a wide area of responsibility and limited personnel which is why you should report abuse multiple times before going on to the next step.

File a report with the stalker’s Internet Service Provider

If you are aware of the stalker's ISP, you may consider this step. The harassing behaviours are likely in violation of the ISP’s Acceptable Use Policy. If the ISP is in agreement, it may result in the termination of a violator's internet service contract. There are pitfalls to this approach - it may result in a temporary suspension of the harassment, there is no monitoring system or database which stops the violator from simply opening up another internet access account with another ISP and continuing the harassment. They may also increase the cyberstalking, if they become upset or enraged by your actions.

Report the offender to a third-party online service organization

Organizations such as Working to Halt Online Abuse (WHOA) are informational resources that may offer more advanced tips on how to stop or gather information useful in a criminal case. They are not based in Canada, but do have information that is applicable. They may also be able to help support if you are having difficulty convincing authorities of the legitimacy of the behaviours as being harassing. They will not be able to report on your behalf, and may not be able to provide referral to local support services.

Report the behaviour/offender to law enforcement

Reporting to the police is the first official step in a criminal investigation. It may lead to a conviction, but this is not a guaranteed outcome. Reporting to the police may also be useful in connecting you with local crisis and support services. As these types of crimes become more prevalent, police are becoming more aware of the cyberstalking behaviours, but individual officers may be unfamiliar with the crimes or technology in question and uncertain how to proceed. It is common to be told to come back if the cyberstalker confronts you offline, or to have police tell you to stop using the technology. There may also be cases where the offender is untraceable, making prosecution difficult.