CYBERSTALKING

PREPARED BY THE CANADIAN RESOURCE CENTRE FOR VICTIMS OF CRIME

This paper is intended as a general guide for people who may become susceptible to crime or for victims that are already involved in the criminal justice system. Please do not hesitate to contact our office if you require clarification, or for a referral to an agency in your community that may be able to provide services to you.

(Revised May 2022)

Canadian
Resource Centre for
VICTIMS
OF CRIME

— Dedicated to Justice —

Canadian
Resource Centre for
VICTIMS
OF CRIME

Table of Contents

Introduction

Cyberstalking is generally used to refer to the use of the Internet, e-mail, or other telecommunication technologies to harass or stalk another person. This could include the intentional behaviour to intimidate victims or make their lives unbearable. It is not the mere annoyance of unsolicited e-mail, it is methodical, deliberate, and persistent. The communications, whether from someone known or unknown, do not stop even after the recipient has asked the sender to cease all contacts, and are often filled with inappropriate, and sometimes disturbing, content. Essentially, cyberstalking is an extension of the physical form of stalking.

There are common characteristics involved with a person who is cyberstalking. This could include tracking the victim's location while also monitoring their day-to-day activities. While also tracking the victim's whereabouts through their social media platforms such as; Instagram, Facebook and Twitter. The cyberstalker could find out information regarding the victim's friends and family, upcoming trips, phone number, home address, etc.

Legislation

Within the Canadian Criminal Code, there are no direct laws connected to *cyberstalking*, but the act can be connected to several different offences, depending on the conduct, including:

- **Criminal Harassment (s 264) –** Criminal harassment consists of repeatedly following an individual or anyone known to them; repeatedly communicating with, either directly or indirectly, the individual or anyone known to them; besetting or watching the dwelling-house, or place where the individual, or anyone known to them, resides, works, carries on business or happens to be; or engaging in threatening conduct directed at the individual or any member of their family.
- **Interception (s 184)** – Interception consists of using a device to purposely intercept a private conversation.
- **Harassing Communications (s 372(3))** – Harassing communications consists of repeatedly communicating with a person by means of telecommunication, without a lawful excuse and with the intent to harass that individual.
- **Uttering Threats (s 264.1)** – Uttering threats consist of knowingly threatening to harm a person, their property, or their pets.
- **Extortion (s 346)** – Extortion consists of using threats, accusations, menaces, or violence to try to compel a person to do something they do not want to.
- **Intimidation (s 423)** – Intimidation consists of using intimidating behaviour to either prevent a person from doing something they are legally allowed to do or to compel a person to do something they do not legally have to do. Intimidating behaviour can include violence, threats, following a person, depriving a person of their property, besetting, watching a person’s workplace or home, as well as blocking or obstructing a person on a highway.

The following are Canadian cases that illustrate what the courts have found as an actionable case for stalking:

- *R v Kordrostami*, several hang-up calls over a few days amounted to harassing behaviour after the victim told the perpetrator to leave her alone.
- *R v Labrentz*, driving around the victim's apartment building as well as repeatedly sending her emails and letters amounted to harassing behaviour.
- *R v Amiri*, the perpetrator repeatedly communicated with the victim by way of text messages, Facebook messages, and phone calls.

Signs of Cyberstalking

Cyberstalking refers to any action in which a perpetrator is using the Internet to harass or threaten an individual. It can involve actions such as:

- Sending repeated unsolicited and/or threatening e-mails to the victim.
- Sending repeated unsolicited and/or threatening e-mails to the victim's friends and family.
- Impersonating the victim online.
- Making defamatory comments about the victim online.
- Leaving abusive messages online, including on social media sites.
- Sending the victim pornography or other graphic material that is knowingly offensive.
- Creating online content that depicts the victim in negative ways.
- Following, watching, and tracking an individual's social media.
- Threatening harm to the victim, their family, friends, and/or pets,
- Doxing involves posting personal information online without the victim's consent such as an address or social insurance number as a means of intimidation.
- Spoofing is a broad term for the type of behaviour that involves masquerading as someone else online or by phone to get a victim to do something.
- Trolling stems from the internet slang 'troll', which is a person who starts arguments or upsets a victim by posting inflammatory, extraneous messages online. A troll aims to provoke other online users into an emotional response often for their amusement.
- Hate speech against a victim by using abusive or threating language that expresses prejudice against a chacteristic that identifies the victim as being a part of a particular religion, race, culture, or sexual orientation.
- Sextortion as an attempt to extort money or get victims to do something against their will by threatening to release embarrassing, personal images or videos about the victim. The compromising images may come from the victim's webcam which is hijacked by malware, or it may be fake imagery such as in sextortion scams.

Impact of Cyberstalking

Unfortunately, victims of cyberstalking may potentially be left with negative impacts related to the crime. These impacts can be psychological or social.

Psychological

- Fear
- Anger
- Paranoia
- Depression
- Post-traumatic stress disorder (PTSD)
- Panic attacks
- Increased suicidal ideation
- Lowered perceptions of control

Social

- Damaged reputation: The perpetrator may impersonate the victim online which could affect the victim's reputation.
- Damaged family relations: Family members may be affected by the victims cyberstalking causing them to create distance between themselves and the victim.
- Loss of work: The victim's work may be affected by cyberstalking which can cause them to lose their job.

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 that 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 are entitled to be able to interact online without fear. You can control your safety and privacy online.

There are programs for your devices, whether that be for your phone or tablet/computer, that is called *Stalkerware*. Stalkerware is a kind of software program that lets another person monitor and record information, without being detected, from your device. This software can be easily bought and installed onto your device without your knowledge. This can happen if someone has access to your device.

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;
- Try to limit the amount of personal information you are posting online;
- Make your social media account private;
- Don't accept friend/follow requests from people you don't know;
- 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 seven letters long because the longer the password, the harder it will be to break (there are more seven letter words in the English language than six or eight letter words);
- Make sure your phone is set to lock quickly while not in use;
- Put a password on your phone- one that isn't easy to guess;
- Be mindful of who you are sharing your devices with;
- Protect your privacy by not publishing or talking about your real name, address, or other contact details as well as not providing location information. Set privacy options to the most restrictive possible;
- Depending on the 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 the 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, instant messaging, 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 see what information is available 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; and
- Take screenshots of any harassing behaviours, especially those that are hard to log into, like video chats (how to do this will vary by device, user manual, or internet search for instructions).

What to do if You Become a Victim of Cyberstalking?*

If you have become a victim of cyberstalking, there are a few options you can take to help:

- Immediately take screenshots of all evidence of cyberstalking that is relevant;
- Contact your local law enforcement agency to see what action can be taken;
- Consider changing your e-mail address, Internet service provider, and telephone number(s);
- Contact online directories to remove yourself from their listings; and
- Let family, friends, and co-workers know 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.

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

Capturing Evidence and Documentation

The following are more formal steps that should be taken if personal measures are not sufficient or the stalking behaviour escalates. If the level of fear or threat increases, or the cyberstalking moves from the online world to direct, in-person contact you would generally take these steps in the order listed below. Dependent on the level of fear and need, you may be taking several courses of action at the same time.

Keep All Devices

Victims may often feel like the best thing to do is get rid of the device that the cyberstalker is contacting them through, but this may escalate the perpetrators controlling and dangerous behaviour. Perpetrators may feel like their control is being threatened and you are removing all access. Instead of getting rid of all devices, some women choose to use a safer computer, device, or phone, but not disable a monitored device to continue collecting evidence. By keeping the device that is connected to the perpetrator, you are also keeping evidence if you decide to report it to the police.

Gathering Evidence

Gathering evidence is important because it allows you to keep a record of what is happening, which can be useful if you decide to report the individual.

Elements that should be documented:

- Emails: It is important to not delete emails or forward them to someone that you trust. Emails contain IP addresses that reveal the originating IP address. If you decided to save, print, or screenshot the email, make sure to save the email header which is where the IP information is stored. The location of the email header may vary depending on what email platform is being used.
- Text messages: Take screenshots of threatening text messages and make sure to include the contact page to show that the messages were sent by the perpetrator, as well as to show the time it was sent. You must capture the evidence immediately because if the perpetrator has access to the same cloud as you, they have access to delete messages.
- Social media/Internet harassment: Take screenshots of harassment on social media, this should be done immediately because posts can be deleted at any time. In addition, if you block someone on certain social media platforms (Instagram) you will not have access to your direct messages with the perpetrator. If you decide to report the harassment to the social media or website company, make sure to document the abuse first.
- Harassing phone calls: Consider recording phone conversations. Note; some provinces have different laws surrounding the use of recorded phone conversations as evidence. In circumstances where a law is in place that you are not allowed to record a phone conversation, make a note of the call, how long it lasted, the time, the date, the location, etc.
- Phone number/Caller ID impersonation: Document your call logs by taking screenshots of the caller ID. Make sure to include the date, time, and the number of the originating call.

Here are some tips on how to document what is happening:

- Document all incidents: It is important to document all incidents, even if you are not sure if you want to report the perpetrator. For each incident, keep track of the date, time, location, identity of the suspect, relationship with the perpetrator (if they are known to you), what caused you to fear for your safety, officer information (if reported), witnesses (if any), suspected technology involved (e.g., phone, email, etc.), and a brief description of what the perpetrator did.

- Save all information related to the event or incident: While some victims may feel tempted to throw away threats that they have been sent, it is important to save them. Taking screenshots or photos of evidence is important for future reference.
- Document only relevant information: Only document information that you think is relevant to the cyberstalking.

When gathering evidence, whether you are going to report it or not, it is important to not post any evidence you have online for others to see, especially the perpetrator. If the perpetrator sees what you are sharing online concerning the evidence you have, it will alert the perpetrator that evidence is being gathered against them, the perpetrator will also have an opportunity to delete any evidence against them, as well as, it may prevent law enforcement from collecting any evidence needed for a criminal investigation.

Report

REPORT THE OFFENDER TO YOUR INTERNET SERVICE PROVIDER

The Internet Service Providers (ISP) can 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 by their abuse and security department. This may not resolve the problem, as the staff is typically a 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. 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 Internet Service Provider, you may consider this step. The harassing behaviours are likely in violation of the ISP’s *Acceptable Use Policy*. If the ISP agrees, 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 the actions taken place toward them.

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 the information that is useful in a criminal case. They are not based in Canada but do have the applicable information. They may also be able to help support you if you are having difficulty convincing authorities of the legitimacy of the harassing behaviours. They will not be able to report on your behalf, and may not be able to provide a 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 may be uncertain about how to proceed. It is common to be told to come back if the cyberstalker confronts you offline, or to have the police tell you to stop using the technology. There may also be cases where the offender is untraceable, making prosecution difficult.

Resources Available

Below are resources that range from being able to locate an email header to resources about technology safety.

Locate an email header: **here**.

Locate a specific IP address: **here**.

How to screenshot on different devices: **here**.

Technology safety resources on how to support women and young people experiencing technology-faciliated violence: **here**.

Technology Safety and Privacy Toolkit: **here**.

To understand technology misuse and safety planning tips and strategies: **here**.

How to secure your accounts online: **here**.

How to choose a secure password for your accounts: **here**.

For stalkerware detection, removal and prevention: **here**.

Contact Us

If you have any questions or concerns, please contact us:

Call: 1-877-232-2610

Email: **crcvc@crcvc.ca**

Text: 613-208-0747

Live chat on our website: www.crcvc.ca

References

BC Society of Transition Houses. (n.d.). Technology Safety Project Resources. Retrieved from https://bcsth.ca/technology-safety-project-resources/?mn=fUw7IqynmL29X98MBH1VgVMQagPhJlI3Gm5d.wj1rPV7K3rx6QFfs

Criminal Code, RSC 1985, c C-46. Retrieved from https://laws-lois.justice.gc.ca/eng/acts/c-46/

Gregorie, T. M. (2001). Cyberstalking: Dangers on the information superhighway. National Center for Victims of crime.

Kaspersky. (2021, August 23). *Tips to protect yourself from Cyberstalkers*. www.kaspersky.com. Retrieved from https://www.kaspersky.com/resource-center/threats/how-to-avoid-cyberstalking

Short, E., Linford, S., Wheatcroft, J. M., & Maple, C. (2014). The impact of cyberstalking: the lived experience - a thematic analysis. *Studies in health technology and informatics*, *199*, 133–137.