INCREASING ACCESSIBILITY TO INFORMATION FOR VICTIMS OF ONLINE CRIME: A RESOURCE GUIDE FOR ADULT VICTIMS

Victims of Violence
340-117 Centrepointe Drive
Ottawa, ON K2G 5X3
www.victimsofviolence.on.ca

We are grateful for support from the Department of Justice-Victims Fund

Department of Justice Canada | Ministère de la Justice Canada

INCREASING ACCESSIBILITY TO INFORMATION FOR VICTIMS OF ONLINE CRIME: A RESOURCE GUIDE FOR ADULT VICTIMS

Introduction

In recent decades, the technological advancements and the vast nature of the Internet have provided many new opportunities for criminal offences to be committed. While technology has rapidly developed and become increasingly accessible, the legislation surrounding these crimes has not been sufficiently updated to reflect the evolution of cyberspace. Additionally, individuals have become vulnerable to online crimes due to the lack of knowledge and resources readily available. This resource guide has been created to help adults that have been victimized by cybercrimes, and educate the online community about preventative measures which can be taken to increase one's safety and security online. The guide will contain a variety of topics which includes; Identity Theft & Identity Fraud, Cyberbullying (Internet Harassment), Cyberstalking, Revenge Pornography, Email & Phishing Scams, Romance Scams and Sextortion. Furthermore, it will explore the current legislation and any relevant, notable cases pertaining to the topics that were previously mentioned.

The overarching principle of cybercrime is defined by "any crime where cyber - the Internet and information technologies, such as computers, tablets … or mobile devices - has a substantial role in the commission of a criminal offence" (Royal Canadian Mounted Police, 2015). The definition is further dissected into two major sections: **technology-as-target (TAT)** criminal offences and **technology-as-instrument (TAI)** criminal offences. The TAT offence targets technological machinery to gain access to unauthorized data and information. Contrarily, TAI offences involve the use of the Internet, as an integral component during the commission of the offence (Royal Canadian Mounted Police, 2015). Technology-as-instrument crimes are personal barrages which can have social and/or financial implications, and results in damaging forms of victimization. Due to the severity and intimacy of TAI crimes, this article will focus on these offences and provide information about the various types of crimes that originate from this area of online illicit activity.

RCMP Cybercrime Strategy

Despite the slowly evolving legislation, the Royal Canadian Mounted Police (RCMP) have developed a cybercrime strategy which aims to proactively approach and combat online illegal acts. Law enforcement agencies have been required to establish and update specialized techniques to understand and respond to cybercriminals. Additionally, police agencies both domestically and internationally need internal collaboration to expand and assist during cyber investigations (Royal Canadian Mounted Police, 2015). It is crucial that police associations and

other legal partners share information due to the "borderless nature of cybercrime" (Royal Canadian Mounted Police, 2015). The domestic and international partnerships have allowed the RCMP "to address common cybercrime threats through various enforcement measures, leading to arrests and charges or other disruption outcomes" (Royal Canadian Mounted Police, 2015). The RCMP Cybercrime Strategy is employed to protect Canadians from online fraudulent and criminal activities.

Identity Theft & Fraud

Although identity theft and identity fraud have similar qualities, there are defining features which differentiate the two criminal actions. Identity theft involves the acquisition of another individual's private information for criminal purposes. Oppositely, identity fraud refers to the "actual deceptive use of the identity information" of another individual (alive or deceased) in relation to various fraudulent activities (Royal Canadian Mounted Police, 2015). The invention of the Internet has enabled and simplified the process for thieves to steal and fraudulently use someone else's personal information. According to the RCMP (2015), thieves will typically seek out the following information:

- Full Name
- Date of Birth
- Social Insurance Number (SIN)
- Full Address
- Mother's Maiden Name
- Username and password for online services
- Driver's license number
- Personal identification number (PIN)
- Credit Card information – numbers, expiry dates and the security code (last three digits printed on the signature panel)
- Bank account numbers
- Signature
- Passport number

Preventative Measures

There are preventative measures which can be taken to reduce the likelihood that an individual will be subjected to identity theft and/or identity fraud. The most important precaution to protect yourself online is to guard your personal information (Canadian Anti-Fraud Call Centre, 2007). Do not provide private information over the phone, Internet or mail unless you've initiated contact and are giving it to a trustworthy, reputable agency. A common tactic used by thieves is to pose as a representative from a financial institution or government agency to deceive their target into disclosing personal information (Canadian Anti-Fraud Call Centre, 2007). If the legitimacy of the agency is questionable, never provide them with any information.

Another strategy employed by hackers is to use 'spyware' to gather information about the target via the Internet. The spyware applications are often concealed within a downloadable software program (i.e. music, videos, and video games) that is available online. Once the software is installed, it tracks the user's activity and that information is secretly transferred back to hacker. In addition to monitoring, the spyware can also collect data from emails, passwords and credit cards (Canadian Anti-Fraud Call Centre, 2007). Therefore, be vigilant about monitoring your online banking statements and accounts. Should you notice any unusual activity on your accounts, report it immediately! Additionally, if you've received phone calls from collection agencies about unfamiliar accounts, or if you've applied for credit and were unexpectedly denied, you should investigate further (Royal Canadian Mounted Police, 2015).

Some additional, quick tips which can increase your safety online include:

- Creating strong passwords which use a combination of letters (upper and lower case), numbers, and symbols;
- Using different passwords for your various accounts;
- Periodically changing passwords, especially in instances where it is known that there has been a security breach on a website;
- Installing security software (firewall, anti-virus and anti-spyware) and updating it when new versions become available;
- Never sending confidential/personal information via email, as it cannot be guaranteed that the server is secure;
- Do not open any attachments and/or reply to any emails that are sent from unsolicited, suspicious or unknown sources (especially in instances where the sender is asking for personal/financial information). If you receive these types of emails, delete them immediately;
- After completing an online banking transaction, make sure you sign out of the website and clear your internet file/caches and 'cookies';
- If you sell, dispose of or give away computer equipment, remember to permanently destroy the personal information that may be saved on the hard drive (Canadian Anti-Fraud Call Centre, 2007).

Online shopping has become popular due to its convenience and efficiency. As a result of this popularity, criminals have manipulated the system and target individuals online to steal their personal information. The following recommendations can help protect individuals that shop online:

- Only shop with trusted merchants;
- Be certain that the website is legitimate. Scammers can create a fake website ("brand spoofing") that looks similar to an official webpage and deceive consumers into providing their personal and financial information. Therefore, you should also verify that you're using the correct URL – including the domain (.com, .ca, etc.);

- Prior to submitting personal information, review the website's privacy policy to understand how your information may be used;
- Before providing your credit card number and/or other confidential information to an online merchant, check that the retailer has a secure transaction system. Typically, Internet browsers will indicate whether you're using a secure Internet link. To check if a website is secure, look for a website address that starts with https://, a closed lock or an unbroken key icon at the bottom right corner of the screen (Canadian Anti-Fraud Call Centre, 2007).

With these minor adjustments to your Internet activity, it can improve your safety online and protect your personal information.

Legislation Pertaining to Identity Theft & Identity Fraud

Although there are no laws dealing specifically with identity theft and identity fraud that occurs online, the legislation in the Canadian Criminal Code does prohibit individuals from using technological devices to acquire and steal another person's private information. The following sections of the Criminal Code indicate and describe the various offences and consequent sanctions for persons who engage in identity theft and/or identity fraud.

Definition of 'identity information'

> 402.1 For the purposes of sections 402.2 and 403, "identity information" means any information – including biological or physiological information – of a type that is commonly used alone or in contribution with other information to identify or purport to identify an individual, including a fingerprint, voiceprint, retina image, iris image, DNA profile, name address, date of birth, written signature, electronic signature, digital signature, user name, credit card number, debit card number, financial institution account number, passport number, Social Insurance Number, health insurance number, driver's license number or password.

Identity Theft

> 402.2 (1) Everyone commits an offence who knowingly obtains or possesses another person's identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.
>
> (2) Everyone commits an offence who transmits, makes available, distributes, sells or offers for sale another person's identity information, or has it in their possession for any of those purposes, knowing that or being reckless as to whether the information will be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.

Punishment

(5) Everyone who commits an offence under subsection (1) or (2)

(a) is guilty of an indictable offence and liable to imprisonment for a term of not more than five years; or
(b) is guilty of an offence punishable on a summary conviction.

Identity Fraud

403. (1) Everyone commits an offence who fraudulently personates another person, living or dead,

(a) with intent to gain advantage for themselves or another person;
(b) with intent to obtain any property or an interest in any property
(c) with intent to cause disadvantage to the person being personated or another person; or
(d) with intent to avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice

Punishment

(3) Everyone who commits an offence under subsection (1)

(a) is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years; or
(b) is guilty of an offence punishable on a summary conviction (Criminal Code, 1985).

Support and Services Available for Victims of Identity Theft & Fraud

If you are a victim of identity theft or identity fraud, please follow the steps below to report the incident and prevent further crimes from occurring. It can be overwhelming and confusing trying to navigate through the system. Therefore, this guide is available to help assist you to ensure you've taken all the necessary steps to rectify this issue.

Firstly, remain calm and create a list of all the identification information that was fraudulently used or stolen. You should keep notes of your interactions with representatives from law enforcement, financial institutions and other agencies. This will assist you should you need to reference any information in the future.

Obtain a copy of your credit report

You will need to contact the following two major credit bureaus and inform them that you've been a victim of identity theft or identity fraud:

Equifax Canada
http://www.consumer.equifax.ca/home/en_ca
Consumer Fraud Division
P.O. Box 190 Jean Talon
Montreal, PQ
H1S 2Z2
1-800-465-7166
514-493-2314

TransUnion Canada
http://www.transunion.ca
Correspondence in English:
Fraud Victim Assistance Department
P.O. Box 338, LCD 1
Hamilton, Ontario
L8L 7W2
1-800-663-9980

Correspondence in French:
Consumer Relations Centre
CP 1433 Succ. St-Martin
Laval, QC
H7V 3P7
1-877-713-3393
514-335-0374 (in Montreal)

Additionally, you'll need to request a copy of your credit bureau report and request that your credit file be flagged with a "fraud warning". This warning will require creditors to contact you directly, prior to opening new accounts in your name and these notices remain on file for six years (Royal Canadian Mounted Police, 2016).

Review your credit reports

Once you've reviewed the reports, contact the creditors and explain that your identity has been stolen or fraudulently used. Furthermore, you must "close any accounts [that] you didn't open and decline any new accounts [that] you didn't request" (Royal Canadian Mounted Police, 2016).

Contact the local police

Report the crime to your local law enforcement agency and remember to get a report number and document it for future referral. Any suspicious information you discover on your credit bureau report should be reported to the police. Often, banks and creditors will need evidence of the

offence to erase the debts associated with the identity theft or identity fraud (Royal Canadian Mounted Police, 2016). Therefore, it is important that you record your police report number. Please be advised that the police are not responsible for reclaiming the money that has been stolen. Instead, their purpose is to investigate the criminal activities and press charges when applicable (Royal Canadian Mounted Police, 2016).

Contact the Canadian Anti-Fraud Centre (CAFC)

You can also report this information to the Canadian Anti-Fraud Centre by visiting their website or by calling **1-888-495-8501**. While the CAFC does not conduct investigations, reporting the incident to them provides CAFC with valuable information which may allow them to identify an affiliation between seemingly unrelated cases (Royal Canadian Mounted Police, 2016). For more information about reporting the crime, please visit their website: http://www.antifraudcentre-centreantifraude.ca/.

Review all of your bank and credit card statements

If you notice questionable transactions on your credit card or bank statements, call the financial institution immediately and file an Identity Theft Statement (ITS). The ITS will help to alert other credit card companies and agencies of your identity theft or identity fraud. In addition, the statement will indicate that you did not amass the debt or charges in question and will provide them with the information required to begin an investigation (Royal Canadian Mounted Police, 2016). Make copies of your Statement, as you will need to submit it to all parties involved. To access the Identity Theft Statement, please visit the Canadian Anti-Fraud Centre's website: http://www.antifraudcentre-centreantifraude.ca/.

Notify credit card companies, banks and other financial institutions and change all of your passwords

According to the RCMP (2016), the following steps are crucial to prevent further fraudulent activities from occurring:

- Contact all financial institutions (credit card companies, banks, etc.) that may have been affected;
- Close all accounts that have been compromised and request that the cancellation be processed as "closed at the consumer's request";
- Acquire a replacement bank/credit card with a new account number;
- Do not re-use your old Personal Identification Number (PIN);
- Never share your banking information with others (PIN, passwords, etc.);
- If you don't have one already, add a password to your account (as this is an additional security feature to protect you)

Cyberbullying (Internet Harassment)

Due to the popularity of social media, cyberbullying has become increasingly prevalent online. Although bullying via the Internet is commonly perceived as an issue among youths, many adults have also been victimized by online bullies. The harasser utilizes technology to intentionally and repeatedly torment, threaten, shame and belittle other individuals (Canadian Bar Association – British Columbia Branch, 2015). Social media sites such as Facebook, Twitter, Instagram, Snapchat and YouTube, alongside blogs, texting and instant messaging are avenues frequently used by cyberbullies. Despite the public nature of this crime, the tormentors are typically anonymous thus it can be difficult to identify and stop them (Canadian Bar Association – British Columbia Branch, 2015).

Preventative Measures

The following steps are precautionary instructions to prevent individuals from being harassed on the Internet.

1. Periodically check your privacy settings on your online accounts

Social media sites are often revising and updating their privacy settings. Therefore, it is important to make sure your profile is as secure as possible by keeping all confidential information restricted from public access (Cyberbullying Research Centre, 2013).

2. Keep your contact information private

Do not share your contact information over social media as you never know who might have access to it (Cyberbullying Research Centre, 2013). Also, do not share your passwords for online accounts and do not leave your device unattended when you're logged onto any sites.

3. Learn Internet etiquette

To avoid possible problems with others in the online community, learn how to interact and interpret social cues and conversations in cyberspace. Avoid writing in all CAPS as this can be perceived as yelling and abstain from using sarcasm because it can easily be misunderstood (Cyberbullying Research Centre, 2013).

4. Do not share inappropriate images or videos

Once the content is sent to another individual, the content could be shared without your knowledge and/or consent (Cyberbullying Research Centre, 2013).

5. Do a Google search of yourself

Occasionally Google yourself as you may find that information you thought was private is actually available on public databases (Cyberbullying Research Centre, 2013).

6. Do not accept friend requests from strangers

If you don't know the individual that is trying to add you as a friend on social media, ignore the request. Many social media sites also give you the choice to block the user, if you wish (Cyberbullying Research Centre, 2013).

7. Do not engage with mean people and be cautious when interacting with strangers online

Do not reveal too much information about yourself to strangers online, because you never know what an individual could do with your personal info (Cyberbullying Research Centre, 2013).

Legislation Pertaining to Cyberbullying (Internet Harassment)

As a result of cyberbullying, there are various legislative provisions which have been extended to prohibit persons from harassing, intimidating or threatening other individuals on the Internet. Most recently, the Canadian government amended the Criminal Code and added a section which criminalizes the act of sharing intimate images without the subject's consent. These Criminal Code provisions are detailed below:

Criminal Harassment

> **264 (1)** No person shall, without lawful authority and knowing that another person is harassed or recklessly as to whether the other person is harassed, engage in conduct referred to in subsection (2) that causes that other person reasonably, in all the circumstances, to fear for their safety or the safety of anyone known to them.

Prohibited conduct

(2) The conduct mentioned in subsection (1) consists of

> **(b)** repeatedly communicating with, either directly or indirectly, the other person or anyone known to them;
> …
> **(d)** engaging in threatening conduct directed at the other person or any member of their family.

Punishment

(3) Every person who contravenes this section is guilty of

> **(a)** an indictable offence and is liable to imprisonment for a term not exceeding ten years; or
> **(b)** an offence punishable on summary conviction (Criminal Code, 1985).

Intimidation

423 (1) Every one is guilty of an indictable offence and liable to imprisonment for a term of not more than five years or is guilty of an offence punishable on summary conviction who, wrongfully and without lawful authority, for the purpose of compelling another person to abstain from doing anything that he or she has a lawful right to do, or to do anything that he or she has a lawful right to abstain from doing,

(a) uses violence or threats of violence to that person or his or her spouse or common-law partner or children, or injures his or her property;
(b) intimidates or attempts to intimidate that person or a relative of that person by threats that, in Canada or elsewhere, violence or other injury will be done to or punishment inflicted on him or her or a relative of his or hers, or that the property of any of them will be damaged (Criminal Code, 1985)…

Uttering Threats

264.1 (1) Every one commits an offence who, in any manner, knowingly utters, conveys or causes any person to receive a threat

(a) to cause death or bodily harm to any person;
(b) to burn, destroy or damage real or personal property; or
(c) to kill, poison or injure an animal or bird that is the property of any person.

Punishment

(2) Every one who commits an offence under paragraph (1) (a) is guilty of

(a) an indictable offence and liable to imprisonment for a term not exceeding five years;
(b) an offence punishable on summary conviction and liable to imprisonment for a term not exceeding eighteen months (Criminal Code, 1985).

Publication, etc., of an intimate image without consent

162.1 (1) Everyone who knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct, is guilty

(*a*) of an indictable offence and liable to imprisonment for a term of not more than five years
or
(*b*) of an offence punishable on summary conviction (Criminal Code, 1985).

Definition of "intimate image"

(2) In this section, *intimate image* means a visual recording of a person made by any means including a photographic, film or video recording,

> **(*a*)** in which the person is nude, is exposing his or her genital organs or anal region or her breasts or is engaged in explicit sexual activity;
> **(*b*)** in respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy; and
> **(*c*)** in respect of which the person depicted retains a reasonable expectation of privacy at the time the offence is committed (Criminal Code, 1985).

The Effects of Cyberbullying

Cyberbullying can negatively impact the health and well-being of the individual being targeted by the online attacks. The psychological and somatic effects of Internet bullying may include:

- Increased risk of depression and anxiety;
- Changes in sleeping patterns;
- Increased feelings of sadness and loneliness;
- Changes in eating patterns;
- Increased risk of suicidal thoughts;
- Decreased interest in activities;
- More health complaints, including physical health (Medical Daily, 2013).

Support and Services Available for Victims of Cyberbullying (Internet Harassment)

If online abuse is causing you to have suicidal thoughts or distress, please visit http://suicideprevention.ca/need-help/ to find a crisis centre near you.

Note: If you reside in the Yukon, the Yukon Distress & Support Line offers anonymous, confidential and non-judgemental assistance at 1-844-533-3030 **(**toll-free, Yukon-wide, nightly from 7pm – Midnight). You can also access services from VictimLinkBC at 1-800-563-0808 (toll-free, 24 hours a day, 7 days a week).

Currently, there are no organizations that are solely dedicated to helping those that have been victimized by online harassment. However, there are resources available explaining how to manage the situation when an individual has been bullied on the Internet, as described below:

1. Report the abuse to the appropriate social media platform(s). If the harassment persists, there is the option to block the perpetrator from contacting you on the website(s). Please see the following section "**Reporting Cyberbullying on Social Media Platforms**" for more information about how to report/block someone.
2. Take screen shots and document all forms of abuse. Therefore should you need to report the incident to the authorities, there is evidence of the harassment. It is especially important to record online harassment because the posts could be removed or deleted by the aggressor.

3. If you fear for your safety, contact the police and report the crime. At this time, you can also include the documented harassment in the police report to support your claims.
4. If you're being cyberbullied by work colleagues, report the incident to the Human Resources (HR) department. Provide them with copies of the screenshots and ask that they be included in your personnel file.
5. Seek legal counsel if you think it is appropriate, because cyberbullying may be considered criminal harassment (Bullying UK, 2017).

Reporting Cyberbullying on Social Media Platforms

How to Report Bullying and Abuse on Facebook

In Private Messages

1. Click on the **gear icon** in the top right hand corner of the message box.
2. Select **"Report as spam or abuse".**
3. Click **Close** on the confirmation message

On a Profile

1. Go to the user's profile
2. Click the **ellipses (…)**
3. Click **Report**
4. Click **"Report this profile"** and **Continue**
5. **Choose a reason** to report the profile and **Continue**
   (You may be asked to provide more information)
6. **Choose the option** to report to Facebook
7. **Go** to https://www.facebook.com/support/ to check the status of your report

To Block and Unfriend

1. Click on the **lock icon** in the upper right hand corner.
2. **Select** "How do I stop someone from bothering me?"
3. **Add** a name or email address
4. **Click** "Block"
5. **Select** the right person with that name
6. **Confirm** the block (Freedman, 2016)

How do I report a Page?

1. Go to the Page you want to report
2. Hover over **… More** below the Page's cover photo
3. Select **Report Page**
4. Choose the option that best describes the issue and follow the on-screen instructions

- If you can't access the Page you want to report, consider asking a friend to report it.

- Facebook will review the Page and remove anything that doesn't follow the Community Standards. Facebook may also warn or disable the person responsible

What happens when I report something to Facebook? Does the person I report get notified?

- When something gets reported to Facebook, they'll review it and remove anything that doesn't follow the Facebook Community Standards. Your name and other personal information will be kept completely confidential if they reach out to the person responsible.
- Please keep in mind that reporting something to Facebook doesn't guarantee that it will be removed. You may see something you don't like on Facebook if it doesn't violate the Facebook Terms.

Can I check the status of something I've reported to Facebook or cancel a report?

- If you've reported something for not following our Community Standards, you may have the option to check the status of your report from the Support Inbox. Please keep in mind that only you can see your Support Inbox.
- From this page, you can:
  -Click on any report to learn more about our policies
  -Cancel a report by clicking on the report you want to cancel and selecting **Cancel Report**
  -See when Facebook takes action on your report and the decision they've made
- Please keep in mind that you can only cancel your report if Facebook hasn't reviewed it yet (Facebook, 2017).

How to Report Bullying and Abuse on Twitter

Report an Individual Tweet

1. Click on the **ellipses (…)** under the tweet
2. Choose **Report** in the drop down menu
3. Choose **"It's abusive or harmful"** from the list of reasons to report the tweet and click **Next**
4. Select a reason why the tweet is abusive and click **Next**
5. Select who is being targeted and click **Next**
6. Choose if you want to block or mute the user and click **Done**

Report an Entire Account

1. Click on the **gear icon** on the top right corner of a user's profile
2. Choose **Report** in the drop down menu
3. Choose **"They're being abusive or harmful"** and click **Next**
4. Choose an option that explains the abusive behaviour and click **Next**
5. Select who is being targeted and click **Next**
6. Select up to five examples of abuse from the bully's tweets and click **Next**

7. Choose if you want to block or mute the user and click **Done** (Freedman, 2016)

What happens after I submit a report?

- Once you have submitted your report, Twitter will review the reported account and/or tweets. Twitter will determine whether the account and/or tweets are in violation of their policies, and will take action (ranging from warning the user, to permanently suspending the account) (Twitter, 2017).

How to Report Bullying and Abuse on Instagram

Report a Photo

1. Tap the **ellipses (…)** at the top right hand corner of a photo
2. Select **Report**
3. Choose **Harassment or bullying** from the list
4. Click **Next** after reviewing Instagram's zero tolerance policy
5. Choose who is being bullied and if you want to block them

Report an Account

1. Tap the **ellipses (…)**at the top right hand corner of a profile
2. Select **Report**
3. Select **I believe this account violates Instagram's Community Guidelines**
4. Choose **Report account**
5. Choose **Posting inappropriate content**
6. Choose **Bullying or harassment.** You'll be taken to a confirmation screen (Freedman, 2016)

How do I block someone?

1. Tap their username to open their profile
2. Tap the **ellipses (…)**
3. Tap **Block User**

What happens when I block someone?

- When you block someone, that person can't view your photos/videos or search for your Instagram profile. People aren't notified when you block them.

How do I report a message that was sent to me or stop someone from sending me messages?

- You can report abusive photos, videos and messages that are sent to you with Instagram Direct:
    1. Open the conversation
    2. Tap and hold the message you'd like to report
    3. Select **Report** (Instagram, 2017)

How to Report Bullying and Abuse on Snapchat

How to report cyber bullying and harassment on Snapchat:

1. Open the Snapchat harassment report form. You can find it here: https://support.snapchat.com/en-US/co/other-abuse
2. **Open Snapchat** and **swipe left** from the home screen to access snaps
3. **Note** the time, sender and content – it may be text, a video or a still photo. Snapchat will ask for this information.
4. If you think it will be helpful, **take a screenshot** of the snap for law enforcement. Note that the sender will be notified that you took a screenshot (Freedman, 2016)

To block a Snapchatter who is your friend follow the steps below:

1. Tap the **gear icon** in the upper right hand corner
2. Tap **"My Friends"** on the Profile Screen
3. **Tap on their name**
4. Tap on the **gear icon below their name** and select **Block** to prevent them from sending you Snaps, Chats or from viewing your Story

To block a Snapchatter who chatted with you follow the steps below:

1. Swipe left on the Snapchatter's name who chatted you to open the Chat screen
2. Tap the triple bar lines (≡)
3. Tap **Block** to prevent them from sending you Snaps, Chats or from viewing your Story

To block a Snapchatter who added you follow the steps below:

1. Tap **Added Me** on the Profile Screen
2. Tap their name, then tap the gear icon next to their name – *or simply swipe left on their name*
3. Press **Block** to prevent them from sending you Snaps, Chats or from viewing your Story (Snapchat, 2017)

How to Report Bullying and Abuse on Tumblr

Reporting Abuse

1. Go to Tumblr's form for reporting abuse (https://www.tumblr.com/abuse?_ga=1.131519503.1894290909.1479756257)
2. Choose **"This content is gross or hateful"** from the list of options
3. Choose **"Malicious speech"** if you're reporting an abusive site
4. **Provide the URL, nature of the abuse, and your contact information,** and then click **Submit** (Freedman, 2016).

What if I receive unwanted messages, reblogs or follows?

Simple: Block the person who's sending them. You can do so from a number of places within Tumblr.

- From your mobile or web dashboard, open the user's blog by clicking or tapping on the avatar, then go to the user menu (the little human), and select "Block."
- From your blog settings page on the web, just click the pencil to edit the blocked users then type in the user that you want to block.
- From post notes on the web, click the three dots that appear when you hover over a reply or reblog caption to bring up the block option. From the app, just tap (iOS) or tap and hold (Android) a reply or reblog caption to bring it up.
- From a messaging conversation, click or tap the three dots at the top of the screen, and choose "Block."
- From your mobile or web inbox, click or tap the three dots at the bottom of the ask box, fan mail, or submission, and then hit "Block" (Tumblr, 2017).

How to Report Bullying and Abuse on Reddit

Reporting a Post or Comment to Moderators

1. **Identify the offending post** or comment
2. Click **report,** located underneath the post or comment title in small gray letters
3. **Select why you are reporting it** and click **Report**

Blocking a User

1. Click the **mail icon** on the top right hand corner of the screen
2. Click **"block user"** underneath a post or message from that user
3. Click **yes** when asked if you're sure (Freedman, 2016).

How to Report Bullying and Abuse on YouTube

Report a Video

1. Click the **"…More" option** next to the Share button underneath the name of the video's creator
2. Select **Report** from the drop-down menu
3. Choose **"Hateful or abusive content"** from the list of issues
4. Pick **Bullying** from the drop-down menu
5. **Add details,** including the time in the video when the bullying occurs and any extra relevant information
6. Click **submit,** you'll get a confirmation

Report a Comment

1. Click the **three vertical dots by the comment** and select **"Report spam or abuse"**
2. Choose **"Harassment or bullying"** and **"This is harassing me"**
3. **Confirm that you want to report the user** (Freedman, 2016)

YouTube

Block users from commenting on your YouTube channel

To block someone:

1. Sign in to your Youtube account
2. Go to the channel page of the user you want to block. It should have a URL like www.youtube.com/user/NAME or www.youtube.com/channel/NAME.
3. Click the **About** tab, then click the flag icon
4. Click **Block user** (YouTube, 2017)

How to block a number on an Android phone

Block calls on your Android smartphone with native features

- The method for doing this will vary slightly according to your specific device and the version of Android that you are using.
- **From the call log -** From the call log, you can disable incoming calls from specific numbers. Select the number you want to block, then hit the 3-dot menu icon in the upper right corner and choose *Add to reject list.* This will disable incoming calls from specific numbers.
- **From your contacts list -** If there's a particularly persistent individual whose number you've saved, blocking them is simple. Just pull up your contacts, select the person you'd like to block, and hit the little button in the right-hand corner that looks like a pencil. Then, tap the 3-dot menu icon in the upper right corner and checkmark the box next to *All Calls to Voicemail*. That contact's calls will now be directed to your carrier's voice inbox.
- **From the settings menu -** One of the most common routes is to pull up your contact list by selecting the phone icon from your home screen. Then tap the three dot menu and choose *Settings > Call > Call Rejection > Auto Reject List > Create.* At this point, Android phones will have a search box that'll appear. Insert the phone number or name of the person you want to block, and that name will be added to the *Auto Reject List (Digital Trends Staff, 2017).*

How to block a number on an iPhone (and iPad or iPod Touch)

- **Phone -** If you're in the Phone app under Recents, tap ⓘ next to the phone number or contact that you want to block. Scroll to the bottom of your screen, then tap Block this Caller.

- **FaceTime** – If you're in the FaceTime app, tap ⓘ next to the phone number or contact that you want to block. Scroll to the bottom of your screen, then tap Block this Caller.
- **Messages** – If you're in Messages, open the conversation, tap ⓘ, then select the name or phone number. Scroll to the bottom of the Info screen, then tap Block this Caller.
- **When you block a phone number or contact, they can still leave a voicemail, but you won't get a notification. Messages won't be delivered. Also, the contact won't get a notification that the call or message was blocked** (Apple Support, 2016)**.**

Criminal Case Involving Internet Harassment

On July 31st, 2014, Robert James Campbell was arrested on 181 charges of online criminal harassment, identity theft and defamation (Dimmock, 2014). Twelve years prior, he was being tormented by his work colleagues, and the bullying had escalated so much so that he resigned from the company. For the following decade, Campbell made it his mission to retaliate against his former colleagues and their family and friends (Dimmock, 2014). A total of 38 victims from Canada, the US and UK were affected by Mr. Campbell's destructive actions (Dimmock, 2014).

His online campaign of harassment began when he created fake email addresses to torment his ex co-workers. He would send emails to their employers with the intention to destroy their reputations by alleging that his former colleagues were child predators, prostitutes, and members of Nazi or white supremacy groups (Dimmock, 2014). Ultimately, he pleaded guilty to 63 of the charges and was sentenced to 6 years in prison (CBC News, 2015).

Although the internet provides a certain level of anonymity, often people forget that their online activities have real consequences. In the instance mentioned above, Mr. Campbell's actions had serious ramifications for those individuals that he tormented and thus he was sanctioned. This case also demonstrates that legislation does extend to prohibit illicit online conduct and creates a legal precedent that Internet harassment will not be tolerated by the Canadian judicial system.

Cyberstalking

The three major components of cyberstalking includes "direct communication through email or text messages; Internet harassment, where the offender publishes offensive or threatening information about the victim on the Internet; and unauthorized use, control or sabotage of the victim's computer" or other electronic devices (Department of Justice, 2017). The societal trend of sharing personal information online through social media sites has increased the ease in which perpetrators are able to access and collect info about their targets. For this reason, offenders can be unrelenting and cause intense distress for their victims, anonymously from the comfort of their own homes. Due to the expansive capabilities of technology, offenders can criminally harass their targets in a variety of ways which include the following:

- "Sending harassing messages (sometimes forged in the victim's name) through email or text message to the victim or to the victim's employers, co-workers, students, teachers, customers, friends or family;
- Gathering or attempting to gather information about the victim, including private information relating to his or her home address, employment, financial situation and everyday activities, or using spyware to track website visits or record keystrokes the victim makes;
- Attempting to destroy the victim's reputation by engaging in 'cyber-smearing', i.e. , sending or posting false or embarrassing intimate information about or, supposedly, on behalf of the victim;
- Tracking a victim's location using GPS technology (on telephones, cameras, and other devices);
- Watching or listening to a victim through hidden cameras or monitoring devices;
- Sending viruses to the victim's computer, such as software that automatically transmits messages over a period of time;
- Creating websites about the victim that contain threatening or harassing messages, or provocative or pornographic photographs;
- Encourages others to harass the victim;
- Constructing a new identity to entice the target to befriend the perpetrator" (Department of Justice, 2017).

The classification system for cyberstalkers is divided into four categories that are founded on the nature of the relationship and their motives for the harassing someone on the Internet. The 4 classifications are listed and described below:

- Vindictive cyberstalkers are the most relentless with their online pursuit. The Internet harassment can be initiated by a wide range of topics anywhere from "a trivial debate to an active argument" and the stalkers employ a large variety of "technological methods" to torment their targets (Department of Justice, 2017). Generally, they have a proficient understanding of computers and other online devices.
- Composed cyberstalkers typically threaten their targets as a means to torment and aggravate their victims. Similar to vindictive cyberstalkers, composed Internet stalkers are experienced and knowledgeable about technology.
- Intimate cyberstalkers utilize email and online dating sites to garner attention and charm their targets. The motives of the perpetrator vary, as he/she could be infatuated with a potential romantic partner, or could be attempting to stalk former partners or acquaintances. This category has the largest spectrum of computer literacy from very low to high.
- Collective cyberstalkers are a group of two or more individuals that attempt to punish a person that they believe has mistreated them. This type of stalker may enlist the help of others by publishing the victim's address online, so the recruits can also harass the target (Department of Justice, 2017).

Preventative Measures

Similar to the previously discussed sections, the preventative measures to avoid being cyberstalked encourage users to enable and update the security features on their computer and social media accounts. Furthermore, it is advised that people limit the amount of personal information that they share online. It is also recommended that computers be updated with the most recent antispyware and antivirus software. If a person is persistently harassing you online, block or report the individual on the respective social media platforms.

Legislation Pertaining to Cyberstalking

An individual that engages in cyberstalking may be charged with criminal harassment among various other offences. Due to the broadly defined concept of cyberstalking, there are a vast number of offences that can be committed. The following sections of the Criminal Code will be discussed in detail below; voyeurism, Internet luring, and unauthorized use of a computer. Depending on the circumstances of the prohibited online activity, an offender could also be charged with distribution of child pornography, counselling suicide, defamation, wilful promotion of hatred, extortion, conveying false messages, intimidation, mischief in relation to data, identity theft or identity fraud (Department of Justice, 2017).

Criminal Harassment

> **264 (1)** No person shall, without lawful authority and knowing that another person is harassed or recklessly as to whether the other person is harassed, engage in conduct referred to in subsection (2) that causes that other person reasonably, in all the circumstances, to fear for their safety or the safety of anyone known to them.

Prohibited conduct

(2) The conduct mentioned in subsection (1) consists of

> **(b)** repeatedly communicating with, either directly or indirectly, the other person or anyone known to them;
> …
> **(d)** engaging in threatening conduct directed at the other person or any member of their family.

Punishment

(3) Every person who contravenes this section is guilty of

> **(a)** an indictable offence and is liable to imprisonment for a term not exceeding ten years; or
> **(b)** an offence punishable on summary conviction (Criminal Code, 1985).

Voyeurism

162 **(1)** Every one commits an offence who, surreptitiously, observes — including by mechanical or electronic means — or makes a visual recording of a person who is in circumstances that give rise to a reasonable expectation of privacy, if

(a) the person is in a place in which a person can reasonably be expected to be nude, to expose his or her genital organs or anal region or her breasts, or to be engaged in explicit sexual activity;
(b) the person is nude, is exposing his or her genital organs or anal region or her breasts, or is engaged in explicit sexual activity, and the observation or recording is done for the purpose of observing or recording a person in such a state or engaged in such an activity; or
(c) the observation or recording is done for a sexual purpose.

Definition of visual recording

(2) In this section, *visual recording* includes a photographic, film or video recording made by any means.

Punishment

(5) Every one who commits an offence under subsection (1) or (4)

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years; or
(b) is guilty of an offence punishable on summary conviction (Criminal Code, 1985).

Internet Luring (Luring a Child)

172.1 **(1)** Every person commits an offence who, by a means of telecommunication, communicates with

(a) a person who is, or who the accused believes is, under the age of 18 years, for the purpose of facilitating the commission of an offence with respect to that person under subsection 153(1), section 155, 163.1, 170, 171 or 279.011 or subsection 279.02(2), 279.03(2), 286.1(2), 286.2(2) or 286.3(2);
(b) a person who is, or who the accused believes is, under the age of 16 years, for the purpose of facilitating the commission of an offence under section 151 or 152, subsection 160(3) or 173(2) or section 271, 272, 273 or 280 with respect to that person; or
(c) a person who is, or who the accused believes is, under the age of 14 years, for the purpose of facilitating the commission of an offence under section 281 with respect to that person.

Punishment

(2) Every person who commits an offence under subsection (1)

> **(a)** is guilty of an indictable offence and is liable to imprisonment for a term of not more than 14 years and to a minimum punishment of imprisonment for a term of one year; or
> **(b)** is guilty of an offence punishable on summary conviction and is liable to imprisonment for a term of not more than two years less a day and to a minimum punishment of imprisonment for a term of six months (Criminal Code, 1985).

Unauthorized Use of a Computer

342.1 **(1)** Everyone is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years, or is guilty of an offence punishable on summary conviction who, fraudulently and without colour of right,

> **(a)** obtains, directly or indirectly, any computer service;
> **(b)** by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system;
> **(c)** uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or under section 430 in relation to computer data or a computer system; or
> **(d)** uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c) (Criminal Code, 1985) .

Support and Services Available for Victims of Cyberstalking

Being targeted by a cyberstalker can take a toll on one's mental health; therefore it is beneficial to seek support from family and friends as well as professional assistance. If you're experiencing any of the following signs, you should consider seeking professional help:

- You're extremely anxious and cannot perform basic daily tasks
- You don't derive happiness from activities or hobbies that were previously enjoyable
- You have difficulty trusting new people that you meet in-person or online, because you're afraid that you'll be cyberstalked again
- You feel personally responsible for the cyberstalking incident (Fight Cyberstalking, 2017)
- Difficulty eating and sleeping
- Having feelings of helplessness

If you know the perpetrator, send that person a message and indicate that any additional contact is unwanted. After expressing your demands in the warning message, do not engage in any further communication with that person. At this time, you should also make copies of all electronic interactions you've had with the individual. These copies can be used as evidence of the cyberstalking and Internet harassment. If the cyberstalking persists and you are fearful for your safety, contact your local law enforcement agency to determine what can be done to eradicate the issue. Also, inform family and friends about the online harassment so they are aware of the situation and can provide emotional support during these difficult times. Finally,

never agree to meet up with the offender in-person as this could lead to a potentially dangerous situation.

Please contact your local Victim Services office, as they can provide referrals to counselling and can assist you during legal proceedings should you decide to report the cyberstalking. To find the nearest Victim Services office, please visit the following link and search your postal code (http://www.justice.gc.ca/eng/cj-jp/victims-victimes/vsd-rsv/index.html). It is important to remember that you are not to blame for the actions of others, and if you're feeling scared and are concerned for your safety, you need to contact the police and report the incident.

Criminal Case Involving Cyberstalking

In 2006, Jonathan Barnes was found guilty of cyberstalking his ex-girlfriend and sentenced to one year in prison. After Cari Benson ended her relationship with Barnes, he made it his personal mission to humiliate his ex-girlfriend. He installed keylogging software on her computer to track her keystrokes which granted him access to her passwords (CBC News, 2006). Also, he created a fake email address and sent nude photos of her to her employer, family and friends (CBC News, 2006).

As the personal barrage continued, he withdrew her from her studies at college and he created fake online dating profiles for Cari (CBC News, 2006). Barnes would communicate with the potential suitors and even encouraged them to go to her workplace. Due to the entire ordeal, Cari had to transfer to a new school, get a new job, and change her phone number and social insurance number (CBC News, 2006).

Ultimately, Mr. Barnes (who previously had no criminal record) was charged with criminal harassment and sentenced to a year in prison. While a year-long jail sentence is rare for an individual without a criminal record, the judge stated that "the cyberstalking in this case has serious, far-reaching effects which were just as bad as physical assault" (CBC News, 2006).

Revenge Porn

Revenge porn is described as the non-consensual distribution of sexually explicit images of individuals. The images are obtained through a variety of means including hacking cell phones and/or computers, using hidden surveillance, and consensually acquiring the images from a romantic partner (Franks, 2017). Once the perpetrator acquires the images, these photos or videos are often shared online along with other personal information about the victim. In turn, the victim is exposed to unwanted attention and criticism from peers and strangers, which can have long-lasting, detrimental effects on the victim. Non-consensual pornography can impact the victims' relationships, education and employment opportunities (Franks, 2017). Due to the personal information revealed online, victims are commonly threatened, pursued and harassed by other Internet users. In some instances, victims have been terminated by their employers, or have been forced to change schools and in the worst case scenario a few have committed suicide because of the relentless harassment (Franks, 2017).

Non-consensual pornography has been adopted as an extortion technique employed by domestic abusers, sex traffickers and rapists. Domestic abusers have threatened to publish private images

as a means of intimidating and preventing their partners from leaving the relationship, reporting the violence or obtaining custody of the children (Franks, 2017). Sex traffickers and rapists use compromising photos and videos to degrade the victims and deter them from reporting the offence (Franks, 2017). While revenge pornography affects both men and women, it is evident that women are more often victims of this type of crime and receive more extreme forms of scrutiny (Franks, 2017).

Preventative Measures

The era of technology has simplified the process of sharing information globally. Therefore, it is important to be safe and protect yourself while on the Internet.

1. Avoid taking any photos or videos of yourself naked or in any compromising positions;
2. If you do take nude photos or videos of yourself, refrain from sharing these images with others;
3. If another individual takes a intimate image of you, ask them to delete it and watch to make sure it's been removed;
4. If someone has intimate photos or videos of you, be persistent in your request to have the images deleted;
5. Do not upload compromising photos onto any websites;
6. Be careful who you send private photos or videos to, as these relationships may end and could result in a vengeful ex-partner or friend distributing your intimate images (DMCA, 2017);
7. Cover the webcam on your computer/laptop when it is not in use.

Legislation Pertaining to Revenge Porn

Non-consensual pornography invades an individual's privacy and is extremely destructive, therefore it is imperative that this behaviour be prohibited and sanctioned, accordingly. Recently, the Canadian government has amended the Criminal Code to include a provision which prohibits people from sharing non-consensual sexually graphic images. The Protecting Canadians from Online Crime Act was implemented to respond to the growing number of cyberbullying cases in Canada, most notably regarding the deaths of Rehtaeh Parsons and Amanda Todd.

Publication, etc., of an intimate image without consent

> **162.1 (1)** Everyone who knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct, is guilty
>
> **(*a*)** of an indictable offence and liable to imprisonment for a term of not more than five years
> or
> **(*b*)** of an offence punishable on summary conviction (Criminal Code, 1985).

Definition of "intimate image"

(2) In this section, *intimate image* means a visual recording of a person made by any means including a photographic, film or video recording,

> **(*a*)** in which the person is nude, is exposing his or her genital organs or anal region or her breasts or is engaged in explicit sexual activity;
> **(*b*)** in respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy; and
> **(*c*)** in respect of which the person depicted retains a reasonable expectation of privacy at the time the offence is committed (Criminal Code, 1985).

Support and Services Available for Victims of Revenge Porn

It is important for victims of revenge porn not to blame themselves for having their intimate images distributed without their consent. The images may be shared within the confines of a romantic relationship or the images may be taken during a sexual assault. In either scenario, the victim is not at fault and instead of being critical; friends and family should provide non-judgemental support and be compassionate towards the individual.

Revenge porn is a serious invasion of privacy that is punishable by law. If you've been the victim of revenge porn, begin by documenting the post so you have it should you decide to take further action. Then, you can report the image(s) on the social media site by referring to the following section **Reporting Revenge Porn on Social Media Platforms**. Due to the seriousness of this crime, you should report this to your local law enforcement agency.

If you need any assistance and support, please contact your local Victim Services agency. To find an organization near you, visit the following link and search the directory (http://www.justice.gc.ca/eng/cj-jp/victims-victimes/vsd-rsv/index.html).

Reporting Revenge Porn on Social Media Platforms

The increasing number of cases involving the distribution of non-consensual sexual material has prompted social media sites to implement guidelines restricting these behaviours. Additionally, social media platforms have created tools that allow individuals to report any pornographic or compromising photos that are shared on their websites.

Microsoft Products – Bing, OneDrive, Xbox Live

- If you find non-consensual pornography on any Microsoft products, please report the images by visiting the following link (https://support.microsoft.com/en-us/getsupport?oaspworkflow=start_1.0.0.0&wfname=capsub&productkey=RevengePorn&ccsid=635734559779544586).
- Watch this video as it explains how to report the images on Microsoft (https://www.youtube.com/watch?v=MHyZ17LM-ss).
- Microsoft will remove the images from the global Bing search engine and will delete the content if it is shared on OneDrive or Xbox Live (C.A. Goldberg, 2015).

Google

- Any non-consensual sexually explicit images that are reported to Google will be deleted from their search results.
- The form for reporting Revenge Porn on Google is available here (https://support.google.com/websearch/troubleshooter/3111061#ts=2889054%2C2889099) (C.A. Goldberg, 2015).

Instagram

- The photo and video sharing site, Instagram, has a zero tolerance stance regarding sharing any non-consensual sexual content on the site. Included in the Community Guidelines, Instagram has a policy which prohibits posting photos or videos that contain nudity.
- Instagram's has an all-encompassing procedure for reporting revenge porn, bullying and/or harassment. To file a report with Instagram, please visit the following link (https://www.facebook.com/help/instagram/contact/584460464982589#_=_) (C.A. Goldberg, 2015).

Facebook

- Facebook's Community Standards section explains that any content that "threatens or promotes sexual violence… [or] images shared in revenge" will be remove.
- The instructions for reporting on Facebook are as follows:
    1. Select the photo or video to expand it
    2. Click **Options** in the bottom right
    3. Click **Report Photo** or if it's a video **Report Video**
- If you're having difficulties reporting, complete this form (https://www.facebook.com/help/contact/274459462613911) or if you're reporting on a mobile device, please visit this link for assistance (https://www.facebook.com/help/1432374603715654/list) (C.A. Goldberg, 2015).

Twitter

- Twitter prohibits users from posting another individual's personal information, which includes not allowing users to share photos or videos without the subject's consent. For this reason, the social media site has created a form for individuals that want to report inappropriate online conduct (https://support.twitter.com/forms/private_information)
- You do **NOT** have to have a Twitter account to report abuse (C.A. Goldberg, 2015).

Reddit

- Any compromising images published on Reddit without the subject's permission is prohibited on the site. To notify Reddit, please send an email to contact@reddit.com and attach a link to the inappropriate content (C.A. Goldberg, 2015).

Pornhub

- Although Pornhub doesn't have a written policy prohibiting users from posting revenge porn, they do have a support page where you can request that images be removed from their site (https://www.pornhub.com/support) (C.A. Goldberg, 2015).

Tumblr

- The Tumblr guidelines bans non-consensual pornography and it can be report here (https://www.tumblr.com/abuse/privacy) (C.A. Goldberg, 2015).

Snapchat

- In Snapchat's privacy guidelines, it states that snaps of sexually suggestive images and snaps of individuals without their knowledge or consent are banned.
- If someone posts revenge porn on Snapchat, please report it to the site by visiting the following page (https://support.snapchat.com/en-US/i-need-help) (C.A. Goldberg, 2015).

YouTube

- Nudity and sexual content is not acceptable on the YouTube platform. Therefore, if there are sexual images posted to the site, you can report the video by following the steps below.

Reporting on Mobile Devices

1. Go to the video you'd like to report
2. Tap **More** ⋮ at the top of the video
3. Select **Report** ⚑
4. Click on a reporting option

Reporting on Computers

1. Login to your YouTube account
2. Below the player for the video you want to flag, click **More**
3. In the drop-down menu, choose **Report**
4. Select the reason for flagging that best fits the violation in the video
5. Provide any additional details that may help the review team make their decision including timestamps or descriptions of the violation.

- There is additional information about reporting available here (https://support.google.com/youtube/answer/2802027).

Flickr

To report revenge pornography on Flickr,

1. Go to Flickr.com on your computer (not on your mobile device)
2. At the bottom of the page that contains the photo or video, click **Report Abuse**
3. Select **Intimate content posted without my consent**

4. Enter your email address
5. In the "What's your problem?" field, let Flickr know that you appeared in an intimate image or video without your consent, and provide any additional details that may assist in their investigation. Please include your full name
6. Enter the word "flickr" in the security field
7. Click **SEND**

Criminal Case Involving Revenge Porn

There have been two notable cases involved revenge porn in Canada. The first case demonstrates the problem with the legislation that inadequately protects victims of online crimes. In November 2011, an 18 year old woman sent her boyfriend nude photos and videos while he was away at university (Csanady, 2016). He had been relentlessly demanding the videos for three months, and finally she complied and sent him the intimate images. Almost immediately after receiving the images, he posted them on pornhub.com (Csanady, 2016).

At the time of her reporting the incident to the authorities, there were no criminal charges that could be laid against the perpetrator (Csanady, 2016). However, the police suggested that she could file a civil lawsuit. After a lengthy court case, the Ontario Superior Court awarded her the maximum compensatory amount and required the defendant pay for her legal fees (Csanady, 2016). The judge recognized the challenges associated with technology and the insufficient laws that protect citizens' privacy online.

In wake of the *Protecting Canadians from Online Crime Act*, a Winnipeg man was the first person tried under the new legislation (Khandaker, 2016). After discovering his girlfriend was being unfaithful, he got intoxicated and posted naked photos of her on Facebook. Ultimately, he was found guilty and was sentenced to 90 days in prison and was prohibited from accessing the Internet for 3 years except for occupational purposes (Khandaker, 2016).

In both instances, the judges implemented harsher punitive sanctions to set a precedent for cases of this nature, to clarify that these actions are unacceptable and will not be tolerated in Canada.

Email & Phishing Scams

One of the earliest ways criminals used online technology to commit offences was through phishing scams. The simplicity and broad reaching effects of this crime allowed it to gain momentum through the community of cyber criminals. With the click of a button, offenders can send an email or text to thousands of potential targets. The content of the messages can range from criminals pretending to be a representative from well-respected business or financial institution, to a person trying to transfer large sums of money to the target. In both scenarios, the perpetrator is attempting "to collect personal, financial and sensitive information" about the victim (Royal Canadian Mounted Police, 2015).

The subject matter of the phishing scam is intended to elicit a reaction. Scammers may use tactics to employ an emotional response or may demand immediate action from the victim. The urgency paired together will convincing text (i.e. official company logos or identifying

information) does lead people to believe that the messages they've received are legitimate (Royal Canadian Mounted Police, 2015). Some commonly used catch phrases include:

- "Email Money Transfer Alert: Please verify this payment information below…
- It has come to our attention that your online banking profile needs to be updated as part of our continuous efforts to protect your account and reduce instances of fraud…
- Dear Online Account Holder, Access To Your Account Is Currently Unavailable…
- Important Service Announcement from…, You have 1 unread Security Message!
- We regret to inform you that we had to lock your bank account access. Call (telephone number) to restore your bank account" (Royal Canadian Mounted Police, 2015).

Preventative Measures

Always be wary of any emails or text messages you receive that request your personal or financial information. Typically, banks and credit card companies will not use these forms of communication to contact you (Royal Canadian Mounted Police, 2015). If you want to verify the legitimacy of an email or text, contact the organization by searching the phone number through a credible source (i.e. previous billing statements, visiting the official website for the organization). Never respond to emails or texts that demand personal or financial information. Additionally, if an email or text message has an embedded link in it, do not click on it as it may contain malware or may bring you to an illegitimate website. And remember to routinely check your online banking statements to verify that all transactions are authorized and authentic (Royal Canadian Mounted Police, 2015). Finally, keep your devices updated with the most recent versions of anti-virus and malware software.

Legislation Pertaining to Email & Phishing Scams

There is anti-spam legislation in Canada that prohibits agencies from sending deceptive or non-consensual messages to individuals. The strict penalties associated with this type of offence max out at $1 million for individuals, and up to $10 million for businesses (Government of Canada, 2015). Although the Canadian government has passed this Act, it is difficult for it to be enforced due to the international origins of many cyber scams. However, it is important to report any incidents of phishing scams (please see the *Support and Services Available for Victims of Email & Phishing Scams* section) to accurately demonstrate how many Canadians are affected by this offence. As the government becomes more aware of the serious and damaging effects of phishing scams, they will be more inclined to further criminalize and sanction individuals and organizations that purposefully deceive Canadians through cyber scams.

Support and Services Available for Victims of Email & Phishing Scams

If you unintentionally respond to a suspicious email or text message and provide personal information, begin by contacting your bank and/or credit card companies (Royal Canadian Mounted Police, 2015). Then, you should contact the two credit bureaus in Canada and have fraud alerts set on your accounts (Equifax Canada – Toll Free: 1-800-465-7166, and TransUnion Canada – Toll Free: 1-877-525-3823). The incident should also be reported your local law enforcement agency so they are aware of the fraudulent activity and can respond to any

impending threats (Royal Canadian Mounted Police, 2015). Finally, the Canadian Anti-Fraud Centre should be notified about the phishing scam.

Complaints can be filed using the online form at fightspam.gc.ca or by emailing spam@fightspam.gc.ca.

Canadian Anti-Fraud Centre
Toll-Free: 1-888-495-8501
Toll-Free Fax: 1-888-654-9426
E-mail: info@antifraudcentre.ca
Website: www.antifraudcentre.ca

Canadian Imperial Bank of Commerce (CIBC)

To report fraudulent activity on your CIBC account, send an email to fraud@cibc.com describing the incident and attaching any emails or text messages associated with the fraud. Alternatively, you can also call CIBC (1-800-465-2422 for Canada & US) to alert them about the unauthorized activity (CIBC, 2017).

Royal Bank of Canada (RBC)

Phishing emails and text messages can be forwarded to the RBC email account (phishing@rbc.com), therefore they can appropriately address the spam. Please be advised that the RBC inbox for reporting phishing emails is automated, thus an RBC representative will not be able to response to incoming messages. If you'd like to speak to a representative about the fraud, please call the RBC support line at 1-800-769-2511 (RBC, 2017).

Bank of Montreal (BMO)

To contact BMO (2017) about suspicious activity on your account, please email (online.fraud@bmo.com) or phone them at 1-877-225-5266.

Scotiabank

If you're a Scotiabank client and you've provided financial information to a scammer, immediately contact Scotiabank at 1-800-472-6842, press 3, then 1 to report the incident. If you've received a fraudulent email or text message but didn't reply, please forward the email onto phishing@scotiabank.com (Scotiabank, 2017).

TD Canada Trust

To notify TD Canada about potential fraudulent activities on your bank account, please see the steps below:

1. Visit the following website (https://www.td.com/privacy-and-security/privacy-and-security/report-online-fraud/reportfraud.jsp) and select the embedded link labeled **Online Fraud message window**

2. Detail the suspicious activities which lead you to believe your account has been compromised
3. Select the **Send Message** icon
4. Send an additional supporting documentation such as scam emails and text messages to phishing@td.com (TD Canada, 2017)

To contact a TD representative directly, please contact 1-866-222-3456.

PC Financial

If you've provided confidential information to a phishing scammer, please contact PC Financial at 1-888-723-8881 to cancel your bank card. By emailing PC Financial at fraud@preschoicefinancial.com, you can describe the situation and include any deceptive emails or texts you received. The information provided to PC Financial (2017) allows them to investigate the incident and warn other customers about the fraudulent messages.

Romance Scams

With the surge of online dating websites, criminals have capitalized on the vulnerabilities of others by extorting them. Scammers will create fake profiles using stolen photos to attract potential victims (Canadian Anti-Fraud Centre, 2016). Once lured, the fraudsters invest a great amount of time to establish a trusting relationship with the target. In most scenarios, the criminal is located abroad but expresses interest in travelling to meet the victim. At this time, the perpetrator will seek financial assistance from the target because of an 'unexpected or urgent' situation which has arisen (Canadian Anti-Fraud Centre, 2016). The amount of money demanded varies for each scenario. The lost wages resulting from romance scams can cause serious financial hardships for the victims. In 2015 alone, there were 990 reports of romance scams and Canadians lost nearly $17 million dollars (Russell, 2016).

Preventative Measures

Although it's a lesser known online crime, romance scams are occurring frequently and it can have serious repercussions for the victims. Therefore, there are warning signs which you should be aware of if you decide to partake in online dating:

- Be cautious of individuals that attempt to quickly initiate a relationship with you, or profess their love and adoration for you early on;
- Be wary of people that claim to live near you but are currently working overseas. Fraudsters will use this tactic as a means to ask for money claiming to be in an 'emergency situation';
- Do not send money to anyone regardless of their reasons for requesting financial assistance (Canadian Anti-Fraud Centre, 2016).
- Be cognizant of broken English or language barriers when speaking with individuals online. This could be key indicator in recognizing a scammer as they will typically claim

to be well educated yet will have spelling and grammatical errors when communicating on dating websites;

- Do not share personal information online, as it may be stolen by a fraudster and in turn be used to create a fake online dating profile;
- Be sure to use reputable dating websites (Canadian Resource Centre for Victims of Crime, 2016).
- Be cautious of people that do not want to communicate on dating sites, and instead promptly insist on communicating through email as fraudsters will often use this technique.

Legislation Pertaining to Romance Scams

There is no legislation which specifically prohibits people from engaging in romance scams. Although, persons that falsify their identity or are knowingly deceptive towards others are guilty of fraud. The Criminal Code provision prohibiting fraud can be extended to romance scams, but it is difficult to charge an individual involved in a romance scam with fraud because often the fraudster resides in another country.

Fraud

380(1) Everyone who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security or any service,

(a) is guilty of an indictable offence and liable to a term of imprisonment not exceeding fourteen years, where the subject-matter of the offence is a testamentary instrument or the value of the subject-matter of the offence exceeds five thousand dollars; or

(b) is guilty

(i) of an indictable offence and is liable to imprisonment for a term not exceeding two years, or

(ii) of an offence punishable on summary conviction, where the value of the subject-matter of the offence does not exceed five thousand dollars (Criminal Code, 1985).

Services and Support Available for Victims of Romance Scams

The deceptive charm of romance scammers enables them to lure and manipulate their targets. Unfortunately, many targets have sent funds to the fraudsters; making it a very lucrative business for criminals. If you suspect that you're the target of a roman scam, please see the instructions below which describe how to manage this type of situation.

1. Firstly, do not feel embarrassed about your current situation because someone took advantage of your generosity and altruistic disposition.
2. Discontinue all communication with the potential scammer.

3. Compile and document all money transfers and interactions that you exchanged with the fraudster, as this will be useful if you report the incident. Additionally, make note of any personal information about the scammer.
4. If you've sent money to the individual, contact the company to see if the transfer can be cancelled before the fraudster attempts to claim the funds (please see the following section ***Western Union and MoneyGram*** for information about canceling a money order).
5. Report the romance scam to the dating website where you met the individual so they can disable the account (please see the section ***Reporting Romance Scams on Dating Websites*** for more information about reporting) (Albo, 2016).
6. File a report at your local police station and notify the Canadian Anti-Fraud Centre at 1-888-495-8501.

Western Union and MoneyGram

Western Union and MoneyGram are popular companies used by scammers when they receive wire transfers. In short, these companies are commonly used because the scammer can remain anonymous and receive payments quickly (Manolescu, 2011). The only identifying information the scammer has to provide is a postal code and picture ID. The fraudster can use any postal code they wish and can get a fake ID to match (Manolescu, 2011). Additionally, the wire transfer can be collected from any Western Union or MoneyGram location in the world. Because the wire transfer isn't associated with the scammer's real address or bank account, the funds are not traceable once they've been collected (Manolescu, 2011). Therefore, these companies provide fast, anonymous, risk-free transactions for fraudsters.

To cancel a wire transfer with Western Union:

1. "On WU.com, log on to your Western Union profile
2. Click the **Menu** icon  and select **History** from the dropdown
3. Recent money transfer activity is presented. Click **Show Details**
4. If your money transfer is not eligible for online cancellation, please contact Customer Care at 1-800-235-0000 (Canada) or 1-800-325-6000 (US)
5. Click **Cancel Transfer**
6. Review the information shown. If you would like to continue, at the bottom of the page, click **Confirm cancel**
7. It may take up to 7 business days for your bank to refund your account" (Western Union, 2017)

To cancel a wire transfer with MoneyGram:

- "If you sent the transaction online and you have an account, log in to your account and find the transaction in your transaction history. There is an option to cancel it on the **Transaction Details** page.

- If you sent the transaction online but do not have an account, use the **Track a Transfer** tool to look up the transaction. There is an option to cancel it on the **Transaction Details** page
- It typically takes 3-10 business days for the refund for a money transfer to appear on your credit/debit card or bank account, but may take longer"
- To contact a MoneyGram representative about a specific transaction, please call 1-800-926-9400 (Canada) or 1-800-922-7146 (US) (MoneyGram, 2017).

Reporting Romance Scams on Dating Websites

Dating sites are dedicated to providing the best possible experience for their users and have strict guidelines for their members to abide by. Therefore, individuals that violate the terms and conditions by engaging in romance scams should be reported to the dating platforms. Once reported, the website can appropriately address the situation which may result in terminating the perpetrator's account.

Match

To report a Match user, select the **Report a Concern** link located on the member's profile or at the bottom of a Match email. When reporting an issue on Match, it remains completely anonymous and the information will not be shared. Once the link has been selected, you have the option to choose and describe your reason for reporting the user. Match offers some examples of scenarios in which it is encouraged to report another member:

- "If a member requests money
- If a member tries to sell you merchandise or services
- If a member tries to offer you a job or another "unique opportunity," especially in another country
- If a member's profile text or email claims they are not actually in the location their profile states (e.g., they are really in Russia or Nigeria)
- If a member's profile just does not add up (e.g., the photo doesn't match the information)
- If a member sends you harassing or offensive emails
- If you know a member is actually married (and not separated) or is a minor
- If you see an inappropriate profile or photos on the site, or if you receive inappropriate photos via email or text message
- If a member behaves inappropriately during or after meeting in person
- If a member violates any other Match policy" (Match, 2017).

OKCupid

OKCupid encourages individuals to report any users that are suspicious or harass other members. To report a user for inappropriate conduct, click the ellipsis (…) icon under the message button on the individual's profile page and then select the **Report** button. To report on the dating app, go to the user's profile and select the icon in the upper right corner, then click **Report.** Once a complaint is filed, it will be sent to the moderation team at OKCupid and they can properly

respond to the issue. Any concerns filed with OKCupid remain anonymous and the member that's been flagged will not be notified who reported them (OKCupid, 2017).

Christian Mingle

To report any misconduct on Christian Mingle, please visit the following link (https://www.christianmingle.com/contactus) to file a report against another user (Christian Mingle, 2017).

Plenty of Fish

Plenty of Fish does not tolerate users that violate their community guidelines. Thus, please report any members that have breached the conditions and the staff will review their suspicious activity and determine the correct course of action. To report a member of Plenty of Fish, select the **Report User** icon at the bottom of their profile (Plenty of Fish, 2017).

EHarmony

To report matches that you believe may be involved in a romance scam, please send an email to matchconcerns@eharmony.com and "include all relevant information such as match name, location and any specific concerns regarding the match in question". EHarmony will also notify you if a match's account has been terminated because they've been reported by another user for inappropriate conduct. It is strongly recommended to discontinue contact with a user whose account has been disabled (EHarmony, 2017).

Tinder

With Tinder, you can report both people you've matched with and people you haven't. To report a user on the app, go to their profile and select the ellipsis (…) icon and click **Report** (Tinder, 2017).

Bumble

Reporting users on Bumble is very simple, just go to their profile, scroll to the bottom of the page and select the **Block or Report** icon. You will have to specify the reason for reporting the individual but it will all remain anonymous.

Sextortion

Sextortion is similar to revenge porn in that there are intimate images that could potentially be shared online. However, extortionists will not automatically post the compromising photos online. Instead, they will threaten to share the images unless the target abides by their pre-determined conditions (Royal Canadian Mounted Police, 2017). The coercive, non-physical threats typically involve demands for money, property or sexual favours. A common method for acquiring the sexually explicit material is by targeting individuals on social media platforms or

online dating sites. After establishing a relationship with the target, the extortionist will convince the target to send him/her photos and/or videos of them naked. Another technique used by extortionists is to encourage the target to contact them via webcam video call services and will ask them to perform in a sexual manner. At this time, the offender will secretly screen capture and record the target. Once the perpetrator is in possession of the intimate content, they will threaten to leak the images online.

Preventative Measures

With the growing number of people using social media and dating sites, sextortion scams have become increasingly common in recent years. To ensure your safety online, begin by only accepting friend requests from people you know (Royal Canadian Mounted Police, 2017). Generally, extortionists will send friend requests or initiate relationships with strangers online, in hopes of luring the targets to pose nude. If a person asks you to perform a sexual act via the Internet, deny the request and end all communication with this individual (Canadian Anti-Fraud Centre, 2017). In addition, you should block and remove the extortionist from all your social media accounts. It is also important that you disable your webcam and keep it covered when it is not in use, because hackers can gain remote access to it without your knowledge (Canadian Anti-Fraud Centre, 2017). Finally, if you are thinking about sending compromising images to someone, "carefully consider who you are sharing [sexually] explicit videos and photographs with" (Canadian Anti-Fraud Centre, 2017). Even if you are sending it to a trusted individual, remember that there is always the possibility that these images could be shared without your consent.

Legislation Pertaining to Sextortion

Due to this being a relatively new type of crime, there isn't specific legislation which addresses sextortion. However, the Protecting Canadians from Online Crime Act along with legislation prohibiting extortion criminalizes the actions of extorting and threatening to share sexually intimate images of others online. Within the Criminal Code (1985), section 162.1 prevents people from distributing sexually explicit images without the consent of the subject and section 346 (1) criminalizes the act of extorting people.

Publication, etc., of an intimate image without consent

> **162.1 (1)** Everyone who knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct, is guilty
>
> **(*a*)** of an indictable offence and liable to imprisonment for a term of not more than five years
> or
> **(*b*)** of an offence punishable on summary conviction (Criminal Code, 1985).

Definition of "intimate image"

(2) In this section, *intimate image* means a visual recording of a person made by any means including a photographic, film or video recording,

> **(*a*)** in which the person is nude, is exposing his or her genital organs or anal region or her breasts or is engaged in explicit sexual activity;
> **(*b*)** in respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy; and
> **(*c*)** in respect of which the person depicted retains a reasonable expectation of privacy at the time the offence is committed (Criminal Code, 1985).

Extortion

> **346 (1)** Every one commits extortion who, without reasonable justification or excuse and with intent to obtain anything, by threats, accusations, menaces or violence induces or attempts to induce any person, whether or not he is the person threatened, accused or menaced or to whom violence is shown, to do anything or cause anything to be done (Criminal Code, 1985).

Services and Support Available for Victims of Sextortion

While an instinctual response when being extorted is to pay the ransom, it is actually recommended that targets not pay the extortionists (Cleveland Police, 2017). In some instances where the requests have been fulfilled, the perpetrators will return and have additional, increasing demands. Instead of paying, stop communicating with the extortionist and document the interactions in which they threaten to post the intimate images. The documentation of the extortion is very important, because it can be used as evidence if you decide to report the incident. After archiving, you should delete and block the extortionist from all social media platforms (Cleveland Police, 2017). Once the offenders have been block, they will be unable to contact you and generally will move on to another target. At this time, you should report the incident to the police. As more and more sextortion cases are being reported each year, it is important that law enforcement agents are aware of the increasing number of crimes occurring online (Barghout, 2015).

If you have already sent money to the extortionist, immediately contact the company (Western Union, MoneyGram, etc.) to check if the money has already been collected. If the money hasn't been collected, cancel the wire transfer and you will be reimbursed. If it's been obtained, "make note of where it was collected from" as this can be used as additional evidence (Cleveland Police, 2017).

The Future of Online Crimes

As technology continues to develop and becomes more sophisticated, it is important that the Canadian Criminal Code be updated to reflect the modern society we live in. Currently, there are

definite disparities in legislation thus permitting criminals to commit egregious acts and not be properly reprimanded and sanctioned for their actions. Subsequently, the lack of legislation for online crimes means that victims are often unable to seek justice because there is nothing that can be pursued legally. Although the Canadian government has implemented the Protecting Canadians from Online Crime Act, it is limiting with regards to the type of online crimes it protects victims from. For this reason, additional statutes need to be created to address the growing trend of cyber crimes. The Canadian government will encounter challenges when drafting the new legislation because it cannot infringe upon Internet users privacy rights. Additionally, due to the borderless scope of the Internet it will be difficult for legislation to criminalize cyber crimes that have international origins. Nonetheless, there needs to be further legal consequences for criminals that attack other individuals on the Internet. To demand change, contact your local MP's office and express your concerns. To find your Member of Parliament, please visit the following link and search your postal code (https://lop.parl.ca/ParlInfo/Compilations/HouseOfCommons/MemberByPostalCode.aspx?Menu=HOC).

While there are many services available for victims of traditional crimes, it is unfortunately not the same for victims of non-conventional offences such as cybercrimes. Since this type of offence is relatively new, there are not organizations in Canada that specialize in this area of crime. Therefore, it is important that victims report their experiences to law enforcement to demonstrate the prevalence of cybercrimes. If law enforcement agencies notice a great increase in number of reported cybercrime incidents, they will be more inclined to allocate resources towards funding programs and services that support and assist victims of online crimes.

In the future, cybercrimes will become more intricate to match the continually evolving technological advancements. As a society, we must start a conversation about the potential risks for Internet users and promote online safety. Internet users should be encouraged to have their privacy settings enabled on all social media and dating websites. Additionally, individuals should be cautious about interacting and meeting strangers online and trust their instincts if they feel that someone is suspicious. At that time, all contact with the stranger should end immediately and the threat should be blocked from all social media platforms. By educating people about cybercrimes, it raises awareness and advocates for the protection of individuals' personal and financial information while using cyber technology.

Conclusion

The rapid evolution of the Internet has provided criminals with the opportunity to engage in a new category of illicit activities via cyberspace. Due to the increasing accessibility of the Internet, criminals remain anonymous and can contact targets all around the world. This evolving branch of crime has a low risk and high reward ratio for perpetrators, and thus has gained popularity among criminals in recent years. The increasing number of cyber criminals paired with the ill-informed general population has resulted in a lucrative category of crime. Since the

majority of individuals are uninformed about the risks associated with cybercrime, this guide was created to educated the masses about preventative measures, legislation pertaining to various online crimes and the services available to victims of these crimes.

The guide discussed numerous topics which included; Identity Theft & Identity Fraud, Cyberbullying (Internet Harassment), Cyberstalking, Revenge Pornography, Email & Phishing Scams, Romance Scams and Sextortion. In all of these scenarios, it is important that the victim reports the incident to police and takes the proper measures to end all contact with the perpetrator. Additionally, the victim should immediately document any information or images that could be used as evidence. Recording the evidence is a time-sensitive issue because at any moment the perpetrator could decide to remove or delete the material from the Internet. Once the content has been removed, it is more difficult to retrieve a digital trace of the explicit or confidential information. In addition to informing victims, the guide ultimately revealed the shortcomings of contemporary Canadian statutes for cybercrime.

Throughout the article, it was evidently identified that current Criminal Code legislation does not adequately protect Canadians from online crimes. While the Canadian government has slowly implemented new laws regarding cybercrime, it remains insufficient and requires further enactment of legal sanctions for individuals that violate the rights of others. In accordance with this, there needs to be more programs and services available to victims of online crimes. While there are traditional victim services, these organizations may be limited in how they can assist victims of cybercrimes because these agencies are, like the general population, less informed about crimes on the Internet. Overall, our society needs to openly discuss the newly emerging branch of online crimes and properly address the issues associated with cybercrimes.

We are grateful for support from the Department of Justice-Victims Fund

Department of Justice Canada | Ministère de la Justice Canada

Sources

Albo, B. (2016). *The Ins and Outs of Reporting a Dating Scam.* Retrieved from https://www.liveabout.com/the-ins-and-outs-of-reporting-a-dating-scam-1022046

Apple Support (2016). *Block phone numbers and contacts or filter messages on your iPhone, iPad or iPod Touch.* Retrieved from https://support.apple.com/en-ca/HT201229

Barghout, C. (2015). *'Sextortion' of Canadian teens spikes 40%, prompts warning.* Retrieved from http://www.cbc.ca/news/canada/manitoba/sextortion-canadian-teens-1.3240470

BMO (2017). *Report Online Fraud.* Retrieved from https://www.bmo.com/home/popups/about/report-fraud

Bullying UK (2017). *The Effects of Cyberbullying*. Retrieved from http://www.bullying.co.uk/cyberbullying/effects-of-cyberbullying/

C.A. Goldberg (2015) *How to Report Revenge Porn on Social Media.* Retrieved from http://www.cagoldberglaw.com/how-to-report-revenge-porn-on-social-media/

Canadian Anti-Fraud Centre (2016). *Romance Scams.* Retrieved from http://www.antifraudcentre-centreantifraude.ca/fraud-escroquerie/romance-rencontre-eng.htm

Canadian Anti-Fraud Centre (2017). *Extortion Scams.* Retrieved fromhttp://www.antifraudcentre-centreantifraude.ca/fraud-escroquerie/types/extortion-extorsion/index-eng.htm

Canadian Anti-Fraud Call Centre (2007). *Identity Theft: Consumer Identity Theft Kit*. Retrieved from http://cmcweb.ca/eic/site/cmc-cmc.nsf/vwapj/Consumer%20Kit.pdf/$FILE/Consumer%20Kit.pdf

Canadian Bar Association – British Columbia Branch (2015). *Stalking, Criminal Harassment and Cyberbullying.* Retrieved from https://www.cbabc.org/for-the-public/dial-a-law/scripts/criminal-law/206

Canadian Resource Centre for Victims of Crime (2016). *Helping Victims of Fraud Recover.* Retrieved from https://crcvc.ca/wp-content/uploads/2011/10/helping-victims-of-fraud-recover_Jan2016_final.pdf

CBC News (2006). *Cyberstalker sentenced to one year.* Retrieved from http://www.cbc.ca/news/canada/cyberstalker-sentenced-to-one-year-1.583770

CBC News (2015). *Robert Campbell sentenced to 6 years for cyberbullying campaign.* Retrieved from http://www.cbc.ca/news/canada/ottawa/robert-campbell-sentenced-to-6-years-for-cyberbullying-campaign-1.3036116

Christian Mingle (2017) *Online Dating Safety Tips.* Retrieved from https://www.christianmingle.com/help/safety/

CIBC (2017). *Online Fraud Reporting and Alerts*. Retrieved from https://www.cibc.com/en/privacy-security/report-online-fraud.html

Cleveland Police (2017). *Sextortion Advice*. Retrieved from https://www.cleveland.police.uk/advice-information/Sextortion.aspx

Criminal Code, R.S.C. 1985, c46, s. 231(6).

Csanady, A. (2016). '*Few things…are more private than a sex video': $100,000 award in revenge porn case a Canadian first.* Retrieved from http://nationalpost.com/news/canada/there-are-few-things-in-life-that-are-more-private-than-a-sex-video-100000-award-in-revenge-porn-case-a-canadian-first/wcm/fb772044-4d76-4076-95b6-0503eff7061e

Cyberbullying Research Centre (2013). *Preventing Cyberbullying : Top Ten Tips for Adults Who Are Being Harassed Online.* Retrieved from https://cyberbullying.org/preventing-cyberbullying-adults

Department of Justice (2017). *A Handbook for Police and Crown Prosecutors on Criminal Harassment: Online Criminal Harassment, Cyberstalking and a Related Typology.* Retrieved from http://www.justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/har/part1.html

Digital Trends Staff (2017). *How to Block Phone Calls on Your Android Phone.* Retrieved from http://www.digitaltrends.com/mobile/how-to-block-phone-calls-on-your-android-smartphone/

Dimmock, G. (2014). *Accused Ottawa cyberbully apologizes: 'I crossed the line'.* Ottawa Citizen. Retrieved from http://ottawacitizen.com/news/local-news/accused-ottawa-cyberbully-apologizes-i-crossed-the-line

DMCA . (2017) *How to stop from being a victim of revenge porn.* Retrieved from https://www.dmca.com/FAQ/How-to-stop-from-being-a-victim-of-revenge-porn

EHarmony (2017). *How do I report matches that I believe may be suspect?*. Retrieved from http://help-singles.eharmony.ca/app/answers/detail/a_id/1031/~/how-do-i-report-matches-that-i-believe-may-be-suspect%3F

Facebook (2017). *Facebook Help Centre.* Retrieved from https://www.facebook.com/help/263149623790594/

Fight Cyberstalking (2017). *Cyberstalking Victims Emotional Support*. Retrieved from https://www.fightcyberstalking.org/emotional-support/

Franks, M. (2017) *Frequently Asked Questions about Revenge Porn.* Retrieved from https://www.cybercivilrights.org/faqs/

Freedman, A. (2016). *How to Report Bullying and Abuse on Facebook.* Retrieved from http://www.tomsguide.com/us/report-abuse-on-facebook,review-3591.html

Freedman, A. (2016). *How to Report Bullying and Abuse on Instagram.* Retrieved from http://www.tomsguide.com/us/report-abuse-on-instagram,review-3600.html

Freedman, A. (2016). *How to Report Bullying and Abuse on Reddit.* Retrieved from http://www.tomsguide.com/us/report-abuse-on-reddit,review-3604.html

Freedman, A. (2016). *How to Report Bullying and Abuse on Snapchat.* Retrieved from http://www.tomsguide.com/us/report-abuse-on-snapchat,review-3603.html

Freedman, A. (2016). *How to Report Bullying and Abuse on Tumblr.* Retrieved from http://www.tomsguide.com/us/report-abuse-on-tumblr,review-3607.html

Freedman, A. (2016). *How to Report Bullying and Abuse on Twitter.* Retrieved from http://www.tomsguide.com/us/report-abuse-on-twitter,review-3596.html

Freedman, A. (2016). *How to Report Bullying and Abuse on YouTube.* Retrieved from http://www.tomsguide.com/us/report-abuse-on-youtube,review-3611.html

Government of Canada (2015). *Canada's Anti-Spam Legislation: Frequently Asked Questions.* Retrieved from http://fightspam.gc.ca/eic/site/030.nsf/eng/00305.html#qB10

Instagram (2017). *Instagram Help Centre*. Retrieved from https://help.instagram.com/547601325292351

Khandaker, T. (2016). *Canada's First Revenge Porn Convict Gets 90 Days in Jail.* Retrieved from https://news.vice.com/article/canadas-first-revenge-porn-convict-gets-90-days-in-jail

Manolescu, D. (2011). *Exposing how scammers use Western Union and MoneyGram for fraud.* Retrieved from https://ecrimeexpertblog.wordpress.com/2011/09/30/exposing-how-scammers-use-western-union-and-moneygram-for-fraud/

Match (2017). *Reporting Inappropriate Behaviour.* Retrieved from http://www.match.com/help/faq/1/20/#holder

Medical Daily (2013). *Adult Bullying: What You Need To Know And How It Affects Your Health.* Retrieved from http://www.medicaldaily.com/adult-bullying-what-you-need-know-and-how-it-affects-your-health-247107

MoneyGram (2017). *Frequently Asked Questions – Canceling a money transfer*. Retrieved from http://www.moneygram.com/us/en/faq

OKCupid (2017). *Moderation & reporting profiles.* Retrieved from https://www.okcupid.com/help/answers

PC Financial (2017). *Communicating Securely.* Retrieved from http://www.banking.pcfinancial.ca/mkt/common/legalinfo/importantnotice-en.html?region=ON&language=en&signinop=OB

Plenty of Fish (2017). *Plenty of Fish FAQ.* Retrieved from http://www.pof.com/HelpCenter/helpCenter_reportUser.aspx

RBC (2017). *Phishing Resource Website.* Retrieved from http://www.rbc.com/privacysecurity/ca/email-and-website-fraud-3.html

Royal Canadian Mounted Police (2015). *Email Fraud/Phishing*. Retrieved from http://www.rcmp-grc.gc.ca/scams-fraudes/phishing-eng.htm

Royal Canadian Mounted Police (2016). *Identity Theft and Identity Fraud Victim Assistance Guide.* Retrieved from http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-eng.htm

Royal Canadian Mounted Police (2015). *Identity Theft and Identity Fraud.* Retrieved from http://www.rcmp-grc.gc.ca/scams-fraudes/id-theft-vol-eng.htm

Royal Canadian Mounted Police (2015). *Royal Canadian Mounted Police Cybercrime Strategy*. Retrieved from http://www.rcmp-grc.gc.ca/wam/media/1088/original/30534bf0b95ec362a454c35f154da496.pdf

Royal Canadian Mounted Police (2017). *Sextortion.* Retrieved from http://bc.rcmp-grc.gc.ca/ViewPage.action?siteNodeId=2077&languageId=1&contentId=49277

Russell, A. (2016) *Canadians lost $16.9M to romance scams in 2015, fraud specialist says.* Retrieved from http://globalnews.ca/news/2528529/canadians-lost-16-9m-to-romance-scams-in-2015-fraud-specialist-says/

Scotiabank (2017). *Online Fraud.* Retrieved from http://www.scotiabank.com/ca/en/0,,2970,00.html

Snapchat (2017). *Snapchat Support.* Retrieved from https://support.snapchat.com/en-US/ca/abuse

TD Canada (2017). *Report Online Fraud*. Retrieved from https://www.td.com/privacy-and-security/privacy-and-security/report-online-fraud/reportfraud.jsp

Tinder (2017) *How do I report someone?*. Retrieved from https://www.gotinder.com/faq

Tumblr (2017). *Community Guidelines.* Retrieved from https://www.tumblr.com/policy/en/community

Twitter (2017). *Twitter Help Centre*. Retrieved from https://support.twitter.com/articles/20169998

Western Union (2017). *Cancel your money transfer for a refund.* Retrieved from https://wucare.westernunion.com/care/s/article/ka2150000009PzHAAU/How-do-I-cancel-a-money-transfer?language=en_US

YouTube (2017). *YouTube Help*. Retrieved from https://support.google.com/youtube/answer/2802268?hl=en