Others' Behaviour

TRAINER RESOURCE

This document is a reference and preparation sheet for the trainer, and a companion to the lesson plan.

The Learning Objectives summarize the knowledge that learners should have gained by the time they reach the end of the module.

The Background and Detail for Trainer provides greater details on the content, and links to references. It will allow trainers to learn more about the topic so they can lead discussions or answer questions confidently without being limited to the classroom content. Each item in the Background supports a section in the Lesson Script.

Learning objectives

> An understanding of the characteristics of harassment and bullying online
> An understanding that predators exist online.
> An understanding of the existence of online fraud online and some common types of fraud
> Ability to find support and report online fraud

Background and Detail for Trainer

1 Harassment and bullying online

1.1 In Brief

The harmful effects of online bullying makes it unacceptable but it is hard to identify. Identifying and talking about bullying can be the first step towards stopping it.

1.2 In Detail

- There is no practical difference between online harassment and online/cyber bullying.
  - The terms are often used interchangeably, although bullying is more frequently associated with school or work environments.[1]
  - Cyber bullying can be defined as "willful and repeated harm inflicted through computers, cell phones, and other electronic devices."
    - Criminal harassment is considered to be a repeated conduct that causes its target to reasonably fear for their safety.[2]
- It is impossible to know exactly how much cyberbullying goes on among teens, but it is likely that at least 20-30% of youth have been victimized.[3]
  - Be careful of the idea that bullying is common or widespread.
    - This idea could lead to people believing that bullying is normal and therefore "not a big deal."
  - One incident of any form of bullying is one too many.
  - The bullying acts that create the harm are various and difficult to classify or identify easily.[4]
  - Repetition might be the most important and easily identifiable element of bullying.[5]
    - The ongoing nature of bullying creates a situation where the target continually worries about what the aggressor will do next; a worry that in itself could be a cause of harm.
    - Being targeted over and over again, even with relatively mild forms of mistreatment, eventually takes a toll.
    - The harm caused by online bullying is sometimes not obvious. However, it is much worse than simply being mistreated, pushed, or generally made fun of.
    - Bullying has never been acceptable or beneficial.

1 https://www.ccohs.ca/oshanswers/psychosocial/cyberbullying.html
2 http://www.justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/har/part1.html
3 http://www.prevnet.ca/bullying/facts-and-solutions
4 see part 1.6 of: http://www.justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/har/part1.html
5 http://www.getcybersafe.gc.ca/cnt/cbrbllng/prnts/cbrbllng-en.aspx

  - There is no truth in statements such as:
    - Boys will be boys;
    - It'll toughen him/her up;
    - It will help him/her grow a backbone so s/he can handle life; and
    - If it doesn't kill you, it'll make you stronger
  - These phrases are often used to minimize, normalize or cope with hurtful behaviour and cyberbullying after it occurs.

All life lessons can be taught better and more humanely in ways other than by enduring bullying.

- What makes a bully?
  - Cyberbullies may:
    - be angry, frustrated or otherwise emotionally distraught, and are simply acting out using the technology at their fingertips.
    - want to avenge a hurt or injury, seek justice or teach a lesson.
    - be victims of bullying themselves.
    - be unable to connect their online behaviour and the offline consequences.
      - These aggressors are sometimes called "inadvertent" cyberbullies because, although their postings were intentional, they intended no harm.
    - not necessarily be those who are mean to others in real life, although this is often the case.
- What are the effects on the victim?
  - They may express emotions such as anger, sadness, frustration, embarrassment, stress, fright, loneliness, helplessness, worry, defencelessness and depression.
  - Depending on the person and circumstance, the impact of anonymity, lack of a safe haven, a constant stream of harmful messages, and embarrassment due to the potentially large audience can be especially strong.
  - They may internalize the hurt and consider self-harm or suicide .
- Responses
  - Making the technology work for you.
    - Block certain people from contacting you online.
    - Change passwords, user names or email addresses.
    - Delete anonymous text messages without reading them.

- Turning away from technology.
    - This is an unrealistic and ineffective long-term strategy.
        - Technology is everywhere and integrated in virtually all aspects of life.
        - Communicating electronically has become the primary way that teens reach their friends even surpassing face-to-face contact in some instances.
        - Technology is an important social and educational tool, as well as a source or peer support.
        - No one should miss out on the benefits technology has to offer because of bullying.
- Learn what your grand/children are doing online.
    - Monitoring and content filtering software might be an option for young children but could be counter productive with older children and young adults.
        - Seek more age specific detailed resources from PREVnet: www.prevnet.ca:
    - Work with them to better understand the technology they are using and its privacy implications and settings.
    - Participate in these environments with them, such as watching YouTube videos together or video chatting with family members.
    - Talk with family about acceptable online behaviour, and make it clear that it is safe to discuss feelings of being harassed.
- Be aware that many victims are unwilling to tell adults about their victimization.
    - Boys and older victims are especially unwilling. If they do tell someone, most would tell a friend, a parent/guardian. Some would tell school staff.
    - Few actually seek help from others. If they do tell, their first choice is a friend, then a parent and lastly a teacher. Willingness to tell school staff or a parent decreases with age.
- There are good resources online that provide more specific information, advice and tools to help learn about and deal with cyberbullying.
    - In particular, we recommend the PREVNet website (http://www.prevnet.ca/bullying/cyber-bullying), a Canadian group that provides excellent resources
    - http://www.thedoorthatsnotlocked.ca/app/en/
    - https://protectchildren.ca/app/en/
    - http://mediasmarts.ca/stay-path-teaching-kids-be-safe-and-ethical-online-portal-page
    - http://www.rcmp-grc.gc.ca/cycp-cpcj/bull-inti/bullres-resinti-eng.htm

- http://www.pensezcybersecurite.gc.ca/cnt/cbrbllng/index-en.aspx
- http://www.getcybersafe.gc.ca/cnt/cbrbllng/tns/index-en.aspx
- https://kidshelpphone.ca/Teens/InfoBooth/Bullying/Cyberbullying.aspx
- http://www.spvm.qc.ca/en/jeunesse/ado-Cyberintimidation.asp

1.3 In Practice

DO take online harassment and bullying seriously.

DO be aware of how family members use the Internet.

DO seek information if you are concerned about someone you know.

2 Predators exist online

2.1 In Brief

Sexual abuse is a danger online. Younger people are at greater risk of becoming victims. Being aware of and supportively involved in their use of the Internet can provide a positive supervisory influence.

2.2 In Detail

- The Internet provides an avenue for predators to contact and abuse vulnerable members of society. This can result in the sexual abuse of young people.
  - Victims may be persuaded or forced to:
    - send or post sexually explicit images of themselves;
    - take part in sexual activities via a webcam or smartphone;
    - have sexual conversations by text or online.[6]
    - physically meet with abusers
  - The effects of the abuse (for example, images or videos) may continue to circulate online long after the sexual abuse has stopped.
    - This makes online sexual abuse particularly harmful, as the torment is prolonged far beyond the initial abuse.
- There is no single risk factor for abuse.
  - Rather, there is a complex interplay of multiple risk factors, and missing protective factors that can decrease a young person's resilience, making them vulnerable to abuse.
  - Adolescents may be at greater risk of unwanted sexual solicitations than younger children or adults.

6 https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/online-abuse/what-is-online-abuse/

    - Adolescents are naturally inexperienced, sensation-seeking, impulsive and risk-seeking.
    - This, combined with a tendency to explore sexual urges, makes them likely to be particularly vulnerable online.

- Predators build relationships with children over time and in many ways.
  - The amount of time this process takes varies from seconds to years.
  - The nature of the manipulation depends on many factors but it is common for the abuser to use flattering language and ask about parents, their schedules and sex early on in the relationship.
    - Offenders may use flattery to make the young person feel special, exploiting their natural need to feel loved and cared for.
      - The person may not feel like that are in an abusive relationship and that the offender is trustworthy.
    - Conversely, an offender may use intimidation and fear as part of grooming, potentially using blackmail as a means of control.
      - Abusers may threaten to send images, video or copies of conversations to the young person's friends and family unless they take part in sexual activity.
    - These means are designed to systematically desensitize and psychologically prepare the victim until they are more likely to engage in sexual activity.
- A parent's involvement and monitoring of the young person's Internet use can be a protective factor against abuse.
  - Young people whose parents oversee their Internet use have fewer negative experiences online than other young people.
  - A young person's awareness of parental Internet monitoring and parental involvement with Internet as well as a supportive relationship with parents and peers can reduce the likelihood of being victimized online.
- Victims may respond to abuse in many ways.
  - They may try To cope through suppression and denial or by reframing the issue.
  - They may seek solace in a variety of ways including social support, working hard, worrying, wishful thinking, self-blame, physical recreation, and keeping to themselves.
  - Children need a supportive structure to reveal their experiences of sexual abuse.
    - Children who suffer severe and frequent sexual abuse tend to disclose belatedly, hesitantly and indirectly, or are afraid or shameful of their parents' reactions.
      - Children who expect negative reactions from their parents delay telling them, and also tend to tell people other than their parents.

  - Children find it difficult to initiate a conversation about something secret, confusing and distressful where there are few opportunities in a family for talking about such themes.

  - Children are sensitive to the needs of their caregivers and fear consequences for their family and the offender.

- When children do disclose, they do so in situations where the theme of child sexual abuse is already addressed or activated.

  - Some children feel it can be difficult to find situations containing enough privacy and prompts for them to share their experiences.

  - Disclosure becomes easier if a child perceives that there is an opportunity to talk, a purpose for speaking, and a connection on the subject has been established.

- To report sexual abuse or find more, visit: https://www.cybertip.ca/app/en/report
- Tools and resources are available at: https://www.protectchildren.ca/app/en/

2.3 In Practice

DO be an involved in your child's Internet use.

DO set boundaries for acceptable behaviour.

DO provide a supportive environment that allows them to talk about abuse

3 Online fraud

3.1 In Brief

There is fraud online. Being aware of common scams can help identify and avoid harm. You can Recognize, Report and Stop Fraud online.

3.2 In Detail

- The ease of communications on the Internet allows scammers and con artists to reach more people more easily.
- Some of their scams use telephone calls, fake websites, email, online messaging etc. to try to convince people to part with their personal information, money or the information of others.
- It is important to be wary of scams, and to take your time and think critically if you suspect a person is trying to trick you.
- Being aware of common scams can help identify cons, but there are many other types of scams and variants of these scams.
  - A Request for Money

- Emergency scams
    - Scammers use social media, the Internet and newspapers to target potential senior victims.
        - A call is made from somebody claiming to be a family member or a close friend advising about an urgent situation that requires immediate funds. Common themes have been that the family member was arrested or got into an accident while travelling abroad. Fees are required for hospital expenses, lawyer fees or bail. Usually, the potential victim is instructed to send money through a money service business like Western Union or MoneyGram.
    - How to protect yourself
        - Confirm with other relatives the whereabouts of the family member or friend.
        - Police, judges or legal entities will never ask you to send money through money service businesses.Never give out family members' names or information to unknown callers.
        - Always question urgent requests for money.
- Romance scams
    - Romance scams involve a criminal with false romantic intensions that gain the affection of their victim to gain access to their money
    - These scams have a profound impact on consumers and cause severe financial harm. In 2014 alone, Canadians lost $13 million to this scam.
        - Fraudsters steal photos and use dating sites and social media to lure potential victims into sending money for various reasons.
        - The fraudsters are willing to develop the relationship over an extended period of time. This increases the trust level between the victim and the fraudster which results in the potential victim usually losing more money.
        - The fraudster will gain the trust of the victim through displays of affection, and will sometimes send gifts, flowers and tokens to prove that their feelings are genuine. While the fraudster is usually in another country, eventually they will say that they want to meet the potential victim in person but can't afford to travel and ask the victim to cover the cost. Variations include the fraudster presenting emergency or urgent situations, such as a sick family member, and seeking financial assistance from the victim for various costs.
    - How to protect yourself
        - Be on the lookout for someone who claims to be from Canada or the US but is working overseas.
        - Be careful communicating with someone who claims to have fallen in love with you quickly.

  - Beware if they claim they are coming to visit you but some situation prevents it from happening;
  - If you are dating online, leave the dating site; the person will usually want to use instant messaging or email.
  - Don't cash any cheques or send the person any money for any reason, whatsoever!

- A Company Suddenly Contacts you
  - Service scams
    - ***Microsoft/Windows technician.***
      - Scammers pretend to represent a well-known computer company like Microsoft, and claim that the victim's computer is sending out viruses or has been hacked and must be cleaned.
      - The scammer will gain remote access to the computer and may run some programs or change some settings.
      - The scammer will then advise that a fee is due for the cleaning and ask for a credit card number to cover the payment.
      - In some cases, the scammer will send a transfer from the victim's computer through a money service business like Western Union or MoneyGram.
      - The result is that the victim pays for a service that was not needed as the computer was never infected.
    - ***Lower Interest Rate.***
      - Scammers offer to reduce interest rates on the victim's credit cards or line of credit.
      - They ask for personal information such as SIN, mother's maiden name, date of birth and the credit card number with the expiry date of the cards they want reduced
    - ***Utility Scams.***
      - Scammers claim to represent the local electric, water or gas company, advising that there is an overdue bill and payment is required immediately or the services will be shut off.
      - The scammer asks for payment by prepaid debit such as a Green Dot Card. Prepaid Debit cards are not the same as a bank account. No photo identification is required and the cards are difficult to trace.

- How to protect yourself
  - Microsoft or any other large computer company will never call you.
  - While utility companies do contact customers by phone from time to time, they will never request a payment by prepaid debit over the phone. Overdue payments would appear on your next month's bill.
  - Call the customer service number on your utility bill. This will ensure you are speaking to a real employee of the real company.
  - Never give out personal information over the phone.
  - Don't be afraid to ask questions.
  - If you feel pressured, never hesitate to terminate a call.

- You unexpectedly win
  - Prize scam
    - Scammers claim to represent "Reader's Digest" or "Set For Life Lottery." Persons are told they have won a prize, and have to provide their bank debit card number, date of birth and in some cases, are asked to enter their PIN into the telephone key pad, in order to collect the prize.
    - Scammers target people who do not use online banking services, and use the financial information to take over the account, which is then used to launder money and proceeds from other mass-marketing fraud scams.
    - Prior to receiving any winnings, the consumer must first pay an upfront fee. No winnings are ever received.
  - Vacation scams
    - Individuals receive a cold call advising that they have won a vacation. Real company names such as Expedia, Air Miles, Air Canada and WestJet have been used. The caller advises the potential victim that they are a preferred customer, and have been awarded a credit or discount on a trip if booked immediately.
    - High-pressure sales tactics are used, and the caller will ask for a credit card number to pay for fees such as taxes.
    - There is no Vacation or Flight.
    - How to protect yourself
      - Any unsolicited phone call advising that you have won a lottery is fake. The only way to participate in any foreign lottery is to go to the country of origin and purchase a ticket in person. A ticket cannot be bought on your behalf.
      - Known lottery and sweepstakes companies such as Reader's Digest and Publisher's Clearinghouse will never ask for money up front before sending a prize.

- Any fees associated with winnings will never be paid through a money service business such as Western Union, MoneyGram or by loading funds to prepaid credit cards such as Green Dot.If an unknown caller tells you that you won a contest you didn't enter, hang up.
- If you receive a call advising you have won a free vacation but have to provide a credit card number to cover taxes before going on the vacation, hang up.
- Check the website of legitimate companies; they usually post warnings about these types of solicitations.
- Never give out personal information or credit card information over the phone.
- If it seems too good to be true…it is.

- Buying and selling online
  - Buying online
    - Every year hot-ticket items like gaming systems and toys sell out in retail stores. Scammers will set up web sites or list these items for sale on classified ads and auction web sites. Consumers pay for the item but never receive them.
    - Warning signs
      - An item being sold at an incredible (almost unbelievable) price.
      - Very low in price compared to other similar items being sold.
      - Use of the word "item" instead of what it is that you are buying (very generic conversation- almost sounds cut-and-paste).
      - Spelling mistakes in the ad or communication.
      - Communication done only via email.
    - How to protect yourself
      - Check the "feedback" of the seller from whom you want to buy. Do not buy from a new seller or a seller with negative reviews.
      - Research the company: verify its physical address and phone number.
      - Deal with companies or individuals you know by reputation or from past experience.
      - Never make a deal outside the auction site.
      - Read the terms and conditions; understand the payment options, return policy and product warranty.

        - Verify the fraud coverage with the payment method you use. Using an Internet Payment Service or paying by credit card is often the most secure.
        - If the asking price of a product is too good to be true… it is.

- Selling online
    - Sellers need to be aware that not all offers to purchase are honest ones.
        - The seller usually receives a reply from a scammer looking to buy their item. The scammer will transfer fake payment(s) to the seller's account, paying with a stolen credit card or with fraudulent cheques. In some situations, the victim loses the item and money due to overpayment by the fraudster or shipping charges for the product.
    - Warning signs
        - Scammers don't try to bargain you down, and may even pay you more to remove add from website immediately.
        - Scammers overpay and ask to send additional funds to a shipping agent.
        - They don't come to check out the product; they don't hesitate to buy.
        - They use the word "item" instead of what the item is that you are selling (very generic conversation—almost sounds cut-and-paste.
        - Payment by cheque or money transfer (PayPal, e-transfer).
    - How to protect yourself
        - Call someone you trust to get a second opinion.
        - Do some research on the buyer.
        - Authenticate payments before shipping the goods.
        - If possible, make the exchange in person (public place, not alone, during the day, etc.).
        - Don't just communicate over email: ask for a phone number (if the buyer won't give it to you, it's a sign of trouble).
        - Take your time; don't rush into anything.
        - Don't feel pressured into doing something you're unsure about.
        - Trust your instincts.

- Counterfeit products
    - You can be scammed when buying online by using websites that appear to sell popular brands but actually sell counterfeit ones.

- Counterfeiters have become proficient in producing websites that have the same look and feel as the legitimate manufacturer's.
- Counterfeit products are far inferior and, in many cases, could pose a significant health risk to consumers. For example, counterfeit jackets have been found to contain bacteria, fungus and mildew.

– Warning signs

- Multiple brands but similar products on one site.
- Items on sale at drastically reduced prices (75, 80 even 90% off).
- Spelling mistakes in website or hyperlink.
- The only real contact point is through email.
- Broken English/general wording (cut-and-paste) when communicating.
- Contact email is from Gmail, Hotmail or Yahoo (manufacturers usually use their company email).

– How to protect yourself

- Do your research before buying anything (return policy, seller's feedback, etc.).
- Call the company's toll-free number. Don't be afraid to ask questions.
- Use your credit card and check your bank statements.
- Avoid clicking pop-up ads and links to "great deals."
- If it looks too good to be true… it is.

3.3 In Practice

DO think critically.

DO be suspicious of urgent requests for money and impossible deals.

DO be confident enough to contact a company yourself to check.

4 Getting support

4.1 In Brief

There are organisations available to help if you think you or someone you know has been a victim of fraud. You can take action if you think you are at risk of fraud, if you have lost a card or have been phished, by calling banks and service providers.

4.2 In Detail

- We all face a constant challenge with fraud online.
- Realizing that you have been exposed to fraud is a good start but there are actions that you can take.

- Anyone can make a mistake; it is nothing to be embarrassed about.
- There are many things that you can do to reduce the harm.
- Changing passwords, checking statements and calling to confirm all help.
- You should always report fraud.
- The Canadian Anti-Fraud Centre is committed to helping you to "Recognize, Report, and Stop Fraud."
  - If you think you or someone you know has been a victim of fraud, contact the Canadian Anti-Fraud Centre at: 1-888-495-8501 or report online at http://www.antifraudcentre.ca.
- If you suspect there has been an attempt at fraud related to a bank account or credit card, contact the bank or card provider immediately. Their contact details are generally listed on their website. Some have been included here for convenience.
  - Bank of Montreal
    - Lost or stolen BMO debit card: 1-877-225-5266
    - Lost or stolen BMO MasterCard Canada & US: 1-800-361-3361
    - https://www.bmo.com/main/contact-us
  - Laurentian Bank
    - 514-252-1846 or 1-800-252-1846 (toll-free)
  - National Bank of Canada
    - 1 888 4TelNat (1 888 483-5628)
    - Greater Montreal area: 514-281-3159
    - Canada and the United States: 1-800-361-0070 (toll free)
    - Outside Canada and the United States: 514-281-3159 (collect call)
  - Desjardins
    - Montreal area: 514-397-8649
    - Canada and the U.S.: 1-866-335-0338
    - Other countries (collect call): 514-397-4610
  - Royal Bank of Canada (RBC)
    - 1-800-769-2511 1-800-769-2555 (online services)
    - 1-800-769-2535 (RBC Express online banking Client Support Centre)
    - RBC Bank (Georgia), N.A.: 1-800-769-2553
    - TDD/TTY: 1-800-661-1275

- Scotiabank
    - 1-800-4-SCOTIA (1-800-472-6842), press 3 then 1 if you are a Scotiabank customer and you believe that you have been a victim of online fraud
- Servus Credit Union
    - 1.877.378.8728
- Tangerine
    - 1-888-SAFE-304 (1-888-723-3304)
- TD Bank
    - https://www.td.com/privacy-and-security/privacy-and-security/report-online-fraud/reportfraud.jsp
        - TD Canada Trust: 1 866 222 3456
        - TD Direct Investing: 1 800 465 5463
        - TD Insurance: 1 877 397 4187
        - Web Business Banking Support: 1 800 668 7328
- Emergency/lost or stolen cards phone numbers for financial institutions:
    - ATB Financial: 1-800-661-2266
    - BMO Bank of Montreal: 1-800-361-3361
    - Bridgewater Bank: 1-866-398-4404
    - Canadian Tire Bank: 1-800-459-6415
    - Capital One: 1-800-481-3239
    - CIBC: 1-800-663-4575
    - Citibank Canada: 1-800-305-7259
    - CUETS Financial: 1-800-567-8111
    - Direct Cash Bank: 1-888-466-4043
    - HSBC Bank Canada: 1-866-406-4722
    - MBNA: 1-800-379-2744
    - National Bank of Canada: 1-888-622-2783
    - Peoples Trust: 1-866-452-1138
    - President's Choice Financial: 1-866-246-7262
    - Royal Bank of Canada: 1-800-361-0152
    - Sears Canada: 1-800-288-9965

    - TD: 1-888-347-3261
    - Walmart Canada Bank: 1-888-925-6218
- American Express
    - Lost or Stolen Card
    - In Toronto: (905) 474-0870
    - North America: 1 800 668-2639
    - International (call collect): (905) 474-0870
- Visa
    - Canada: 1-800-847-2911, http://www.visa.ca/en/aboutcan/contacts.jsp

4.3 In Practice

DO Report fraud to the Canadian Anti-Fraud Centre.

DO contact your bank if you suspect fraud related to your bank or credit card.

Glossary of Terms

Canadian Anti-Fraud Centre (CAFC)	The central agency in Canada that receives online Internet fraud complaints.
Cyberbullying	Willful and repeated harm inflicted through computers, cell phones, and other electronic devices.
E-transfer	A method of sending or receiving money online by Interac.
Money Service Business	A company that allows you to send money to another person somewhere in the world
Paypal	A company that allows for transfer of funds to other people online.
Pin	Personal Identification Number.
Pop-Up Ad	An advertisement that opens in a new browser window, often popping up into view.
Scam	A dishonest or deceptive scheme usually for criminal purposes.
Scammer	A person who scams.
Smartphone	A phone that operates much like a computer and is able to browse the Internet and install applications.
Webcam	A video camera that is able to transmit video signal over the Internet.
YouTube	A website (youtube.com) that provides access to video content.