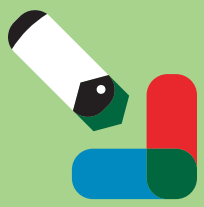
Grades 7-12

Safe Communication Online

ROGERS cybersecure catalyst



We use technology primarily to communicate with each other. We spend a lot of time on our devices chatting with friends, commenting on posts, sharing pictures of a meal or a vacation, using instant messengers (IMs) to stay in touch, and creating group chats to stay close to our community. But what does it mean to communicate online safely? In addition to communicating with friends and acquaintances, many social media platforms and mobile apps allow you to have conversations with people you've never met in-person, and sometimes it's hard to know who's on the other side of the screen or what their intentions are. The key to staying safe online is to limit the amount of private information you share publicly, as strangers may try to use this information to cause harm. Harm can come in the form of personal attacks; someone pretending to be someone else so they can manipulate you, gain access to your personal data or, in some cases, hack into your account(s).

This resource is meant to empower you by providing information on how to recognize the potential risks that come with communicating online, and how to practice safe online communication by making smarter choices.

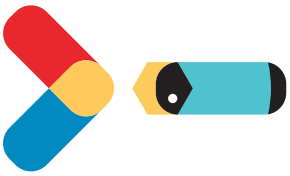
DEFINITION

Be on the lookout for *these* online

- **Exploiters:** They'll often try to look and seem like they're "normal", decent people – but in reality, their intention is to do harm. Exploiters come from all backgrounds and walks of life – and, at first interaction, can be very difficult to spot. Online exploiters typically want something and will try to manipulate you to get it.

- **Online safety risk factors:** Exploiters usually seek out and target people who are more open about sharing their personal thoughts and feelings online. While being vulnerable can be a positive behaviour offline, expressing vulnerability online can provide online exploiters with opportunities for manipulation. One of the easiest and most effective ways to be safe online is to keep your personal life out of public view. Be cautious about what you share, and be mindful of how it may expose you, by using platform settings to manage which audiences can view personal content and what content should be shared publicly. This allows you to share and communicate with people that will be respectful of your personal life and boundaries, and prevents exploiters from having access to your personal information.

- **The White Knight:** One of the ways exploiters manipulate online is by using multiple fake accounts – for example, one account to bully and the other to offer support. A bully account on social media is used to harass, insult and/or demean someone. The White Knight might publicly post offensive messages, and/or hurtful pictures or memes, in order to get their target and others to respond. The White Knight will then use another account to respond to the bully's posts, pretending to stick up for the victim. The White Knight does this to gain trust and attention. The White Knight is pretending to be kind and understanding – but the White Knight's goal is to get closer to the victim, to get personal, so they can manipulate their victim and get access to the victim's information, or convince the victim to meet in-person.



Exploiter:
Someone who takes advantage of other people or their information for their own profit or advantage.

How are you at risk while online?

While we may have the following feelings sometimes, exploiters will often seek out and target you if, in that moment, you're:

- **Feeling insecure about yourself or lacking confidence.**
- **Feeling lonely, or have fewer friends and social groups.**
- **Have limited or complicated family relationships, or simply don't share a lot of information with your family members; exploiters may pretend to understand your life and circumstances.**
- **Still finding your way through life and discovering who you are. Such individuals tend to reach out to others for help or advice, and exploiters use that as an opportunity to provide "guidance". You shouldn't trust just anyone's words or intentions.**

B RELEVANCE

Once an exploiter identifies a person who's feeling vulnerable, they begin trying to befriend and get closer to that person, and gain their trust. Exploiters are good at spotting people who are having a bad day or going through a rough time in their life, or simply feeling lonely. While we all may have these feelings at some point in our lives, exploiters are quick to notice these emotional shifts in others and will try to take advantage of the situation. This process can take an exploiter as little as a few minutes or as long as several months.

Be wary when someone you don't really know...

- Responds to you or your posts with complimentary comments, or starts asking seemingly harmless questions. Potentially, your responses could provide exploiters with details that can be used to find out more about you, or gain access to sensitive information.

- Says they share many or all of the same interests and opinions as you.

- Tries to normalize a relationship that may otherwise be considered odd given the circumstances (e.g., they may be much older than you are or try to form an early romantic relationship). Remember these cues and that such actions can be questionable.

- Pushes you to participate in conversations that start to get too personal or asks you to do something that makes you uncomfortable. This is not okay, and you shouldn't feel pressured to respond.

- Asks to be able to see you, first through requesting pictures, then perhaps through video chat, and eventually even pushes you to meet them in-person. Remember that this can be very dangerous and you should be extremely careful. Whenever you're unsure, ask a parent/guardian or trusted adult for advice.

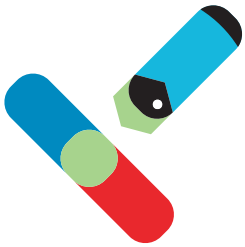
Reflect on your understanding:

Why is it dangerous to post personal and private information online? How can exploiters use this in a negative, malicious way?

Online lures to watch out for

- Someone you don't really know trying to take advantage of your good nature.
- Someone you don't really know promising you things that are too good to be true.
- Someone you don't really know says they know you, your friends or family when they don't. That's why it's important to be mindful of what you share online – and with whom!

Online Lure:
A situation where an individual communicates with someone else, usually a younger person, through technology (like texting or DMs) with the intention of causing them harm.



Cyberstalking

Someone following you on social media is not considered cyberstalking, but if they're using that information to track other aspects of your life – virtual or real – it can be considered dangerous. Keep a lookout for these two common methods used by cyberstalkers:

Cyberstalking:
Typically involves monitoring someone's online activity and/or using connected devices to send ongoing communication, with the intention of harassment or intimidation, causing discomfort or even inducing fear.

- **Catfishing:** Catfishers often pretend to be someone else and will create multiple fake identities online, using fake names, pictures, affiliations, etc. Disguised online, they will lure their victim, who will believe they're someone else. Once they have access to you, they may start tracking your movements online.
- **Phishing:** A fraudulent attempt or scam perpetrated by an Internet user to get private or personal information to use illegally. Cyberstalkers may ask you what at first glance may seem like harmless questions, they get access to information that can be used to track more personal information. This could reveal your travel plans, who you may be going with, and even provide them access to your specific location.

CALL TO ACTION

Trust your gut

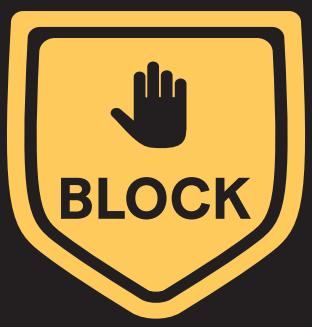
Trusting your gut means believing in your instincts or your immediate understanding of a situation – like when you hear people say "you just know". Most people, unfortunately, have experienced a weird or creepy encounter with someone while out in public. Maybe the person was staring at you too long, stood too close to you or smiled in a strange way. Similar actions can take place online, they just happen differently. Someone may compliment a photo of you in a very personal way, post comments on your profile on an ongoing basis or start friending your friends. Occasionally, exploiters will ask that you refrain from sharing information about them with others; or start asking you to share your secrets with them, but not with your family and friends. This should be a red flag and alert you that something is wrong.

When communicating with others online, you need to be mindful of the situations you place yourself in. It's harder to tell someone's true intentions over a text message than it is in-person. If the situation seems even a little strange, you need to take a step back and consider what's really going on.

Remember this:

Any time someone makes you feel scared or uncomfortable, you need to...

Stop speaking with the person immediately and don't feel the need to explain your reasoning for not replying.



Block the user, but DO NOT delete any of the messages that were exchanged. Share those messages with a trusted adult.

Talk to a parent/guardian or trusted adult immediately. They'll be able to help you evaluate if the potential exploiter's intentions and actions are acceptable.

Location settings

Your mobile devices record your precise location whenever you take a picture or record a video, and can even reveal where you are when you post a comment or image. When the location setting is set to be active on your devices, your media and posts can reveal sensitive details about your location if someone has access to them. Not all social media platforms remove your location data, so the best way to keep your current locations private while posting is to turn off the location services on your devices.

Did you know?

Images and videos contain additional information or descriptions in the background of your image, video or file called metadata; this can include your name and location! Whenever you share these files directly with another user, you're also sharing this personal information.

ACTIVITY 1

Activities are a useful way for you to test and demonstrate your knowledge on the topic covered in this resource.

Assessing Readiness

Reflect on the following questions, or discuss your answers among classmates, family or friends. What would you do if...?

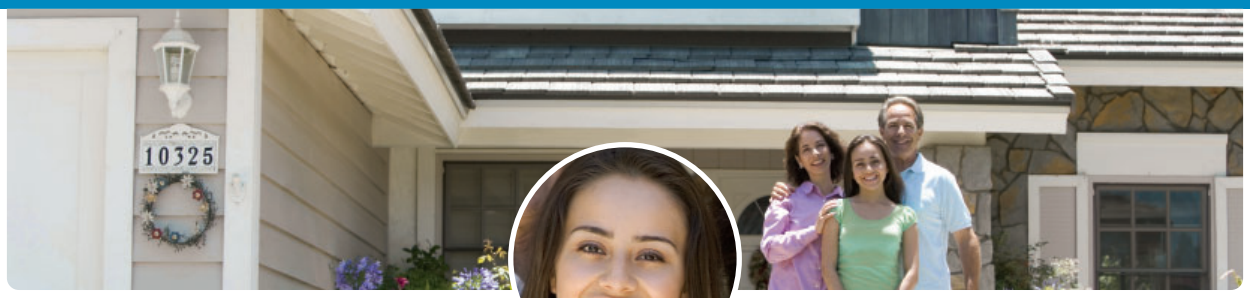
Other than your parents/guardians, who else could you go to for help?
Use this opportunity to identify adults other than your parents/guardians who you know you can trust.

1. **Example:** My soccer coach, Mr. Graham
2.
3.
4.
5.

ACTIVITY 2

Privacy 101

Take a look at the social media profile below; this is an example of a profile when viewed as Public (easily found via a simple Google search). Based on what you've learned in this resource, circle what information is too much information and could potentially help an exploiter strike up a fake friendship.



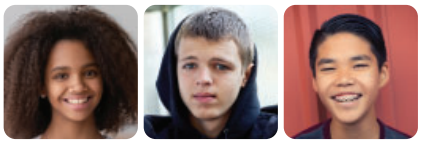
Kiara Reddy

Intro

- Lives in **Mississauga, Ontario**
- Studies at **Cawthra Park Secondary School**
- Works at **PetSmart**
- In a relationship with **Tom Parker**
- Born on **July 11, 2003**

Friends (127)

See all



Simone Jones | Matthew Miller | William Min

Kiara Reddy is at **Lakefront Promenade Park**
October 12 at 8:12 am

Love my morning walks with Lucy!

46 | 9 Comments

Kiara Reddy is feeling sad.
October 14 at 7:12 pm

Missing my best friend. Visit soon, **Amber Foster**!

28 | 7 Comments

Kiara Reddy is **eating dinner** at **Thyme Ristorante**.
October 18 at 6:24 pm

FOR MORE INFORMATION

For more information on cybersecurity, or to continue the conversation and learning process, visit the Canadian Centre for Cyber Security website: https://cyber.gc.ca/en/

Kids Help Phone:

Contact by text message at 686868 or by phone at 1-800-668-6868 from across Canada, 24 hours a day, 7 days a week; or access their resources online: kidshelpphone.ca

ROGERS
cybersecure
catalyst