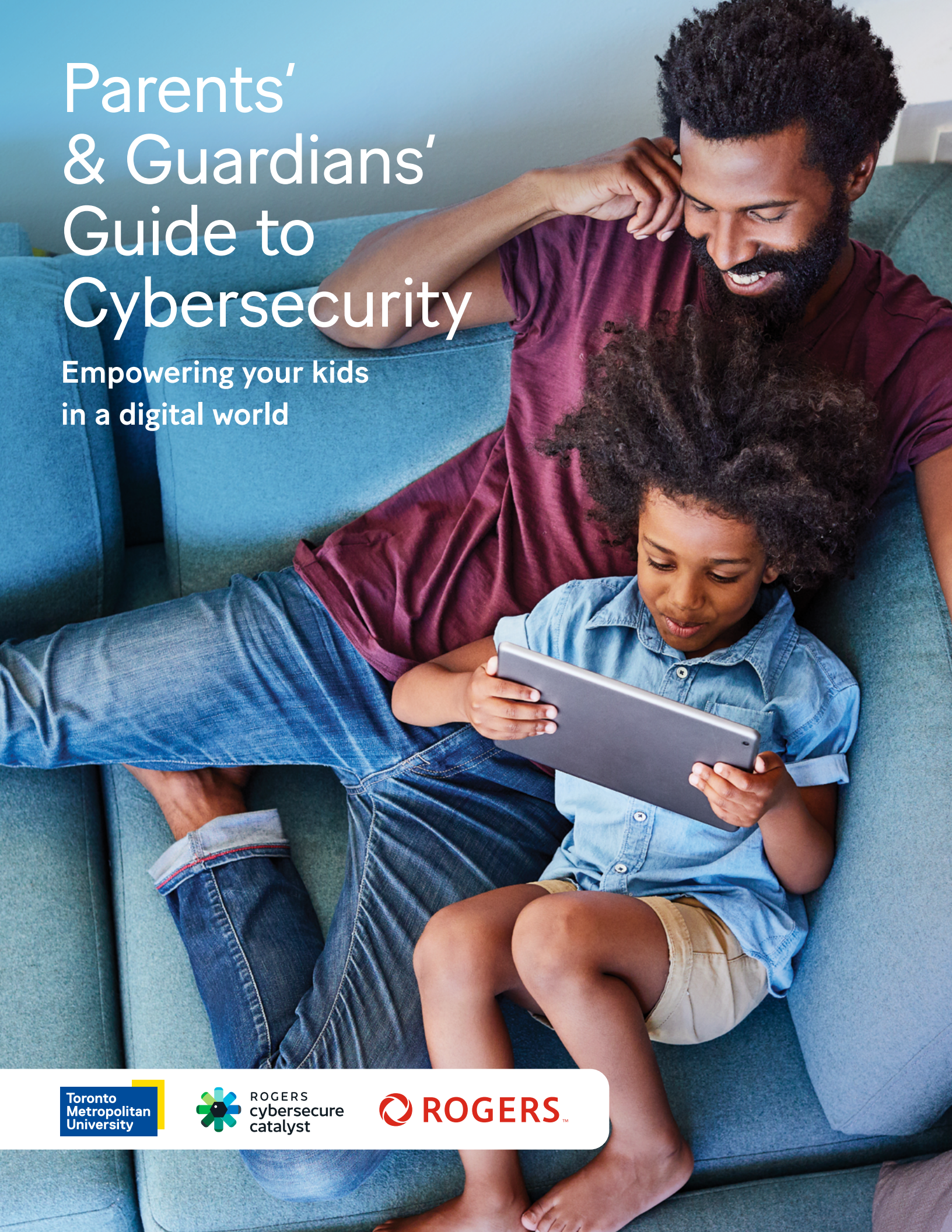


Parents' & Guardians' Guide to Cybersecurity

Empowering your kids in a digital world

Toronto Metropolitan University

ROGERS cybersecure catalyst

ROGERS

The Rogers Cybersecure Catalyst is dedicated to empowering Canadians to seize the opportunities and tackle the challenges of cybersecurity. Nobody has more to gain from our increasingly online world than our youth. The internet is an extraordinary tool for education and communication, and our younger generations will grow up with access to more knowledge than any generation before. They will have new platforms to express themselves, learn about the world around them and chat with friends nearby or on the other side of the globe. Accompanying these extraordinary benefits are real risks associated with the Internet. While these risks are important, there are common-sense strategies that parents and children can use to stay safe.

Our hope is that this guide will be a helpful tool to keep our youth and families secure as they reap the benefits of our digital world.

Charles Finlay
Executive Director
Rogers Cybersecure Catalyst

Toronto Metropolitan University

ROGERS cybersecure catalyst

Rogers Cybersecure Catalyst is Toronto Metropolitan University's national centre for training, innovation and collaboration in cybersecurity. Headquartered in Brampton, Ontario, the Catalyst empowers Canadians and Canadian businesses to seize the opportunities and tackle the challenges of cybersecurity. Through its ground-breaking training and certification programs; unique commercial accelerator for Canadian cybersecurity scale-ups; first-of-its-kind cyber range; wide-ranging public education programs; and influential policy development platform, the Catalyst helps drive Canada's global competitiveness in cybersecurity.

Technology and the internet have transformed our lives—allowing us to connect instantly with family and friends in all corners of the world. From online learning to remote working to social media, the digital world has opened so many doors and opportunities for kids.

As a parent, it can be a bit of an obstacle course, trying to keep up with the latest trends, apps or tools while guiding your kids and teaching them responsibility, respect, kindness and self-confidence. And unfortunately, there's the tougher side of the digital world—the risks and dangers including cyberbullying, malware, misinformation or inappropriate content.

As a cybersecurity professional, I've encountered the same worries and concerns when it comes to teaching kids about cyber safety, which is why I'm so excited to partner with the Rogers Cybersecure Catalyst to develop this handbook for parents and guardians.

This resource is dedicated to helping you navigate those conversations, moments and lessons around online safety.

This guide will help to spark that initial discussion with your kids and share insights and tips to get you started. The most important lesson I've learned is that **cyber safety is a journey**–with ongoing discussions and the occasional role reversal. Sometimes, our kids are the best teachers to help us understand what apps they're using, what they're learning or how they're using their devices.

I hope this guide helps you feel empowered. You're not alone.

Together, we're building the next generation of leaders!

Sundeep Sandhu
Vice President, Cyber Security
Rogers Communications

ROGERS™

Rogers is a leading Canadian technology and media company that provides world-class communications services and entertainment to consumers and businesses on its award-winning networks. The founder, Ted Rogers, purchased his first radio station, CHFI, in 1960. Today, Rogers is dedicated to providing industry-leading wireless, cable, sports, and media to millions of customers across Canada.

Contents

A Look at What's Included

* Key cybersecurity terms will be ***underlined*** throughout the guide—you can find their meanings in the glossary section.

6 Tips
Starting the Conversation

Talking to your kids about online safety is the first step to keeping your family protected. But **how** do you start that conversation?

1 **Stay Current:** Keep up with rapidly changing technologies, and the apps, online games and social media platforms kids are using.

How? Try this: Who better to educate you than *your own kids*? Ask them to show you their favourite app, how to use it or what they like about it. You get to learn what your kids are doing online, and they benefit from the increased safety and security of your supervision. This also provides an opportunity to ask questions that may relate to their safety and security.

2 **Lead by Example:** In addition to being upfront about your expectations with your kids, you should also walk the talk. Make sure you follow the same rules and best practices you put in place for them.

How? Try this: If you're limiting screen time at home, choose a time when the whole family will be screen-free (e.g., during mealtimes, when guests are over, or when going for your evening stroll)—yes, even you!

3 **Build a partnership:** By involving kids in discussions and decisions about technology, you'll establish trust and respect.

How? Try this: Collectively setting up family rules or developing a family contract for using devices (e.g., using devices in open, high traffic rooms in the home instead of bedrooms and bathrooms).

Much of the advice offered in this guide is great for tweens and teens; however, it's never too early to start the conversation. Be sure to use age-appropriate examples and language when talking with younger kids.

6 Tips

Starting the Conversation

continued

4 **Encourage critical thinking:** Curiosity is an integral part of growing up. In today's increasingly digital world, the internet is a leading source of information that can answer virtually any question in a matter of seconds. But the internet also contains information that's not suitable for kids and teens. It's also important to be aware of potential dangers from free apps and tools, and to think critically about offers that seem too good to be true.

How? Try this: Foster critical thinking at home by encouraging discussions about how and when the internet should be used. When kids become more critical about what they see and read online, they're more likely to become responsible digital citizens.

5 **Balance the conversation:** Be the voice of reason, not fear.

How? Try this: Balance online safety conversations by introducing positive and interesting technology stories. For example, it's great that video-calling apps like Skype and FaceTime allow us to connect with friends and loved ones—but posting videos publicly on social media could be dangerous if it includes private information such as full name, school, street address and more. It's not just about letting them know what they shouldn't do, but ***why*** this information should never be shared online and the potential impacts if it is shared.

6 **Provide support:** Although these types of conversations can seem daunting, they're a good opportunity to let your kids know that they're not alone.

How? Try this: Discuss how kids can get help and from whom (build a network of ***trusted adults*** to provide support and monitor safety), and emphasize that they shouldn't fear your reactions or losing technology privileges if they experience some sort of device risk or encounter a suspicious person online. Positively reinforce that your priority is to protect them, in-person and online.

Remember that talking about cybersecurity and cyber safety is not a one-time conversation. As technology advances, your kids get older and their use of connected devices and interests change, the discussion should be revisited often.

Quick Guide

Keeping Your Kids Safe

Technology offers your kids many opportunities to learn and have fun, but it's important to recognize that with these opportunities come risks. Use the following guide to understand and explain to your kids how to recognize, prevent and respond to potential online safety risks.

What are the risks?

Identity theft

Identity theft is when a person's private identifying information is fraudulently acquired. Even if criminals don't use this information right away, they'll have it to use later or sell to others.

Bonus tip: don't use the same password across multiple accounts; when changing passwords, change the entire password; and never share passwords with friends.

What can you do?

Limit the amount of personal information shared online

Your kids should be aware of the potential danger of posting personal information. Avoid posts that can identify them, including their full name, school, city, address, date of birth, etc. Personal information is more than just your name—it can be revealed by taking selfies in a school bathroom or sharing a live location.

Password safety

Passwords protect online accounts and prevent others from accessing the personal and private information stored in online profiles. A simple rule to remember is "longer is stronger". Recommended minimum length is 15 characters, and include a variety of characters, such as upper case (ABC), lower case (abc), numbers (123) and symbols (!@#$). Alternatively, ***passphrases***, or a password composed of a sentence or combination of words, can be used as they are easier to remember but just as strong as a complicated password.

Enable multi-factor authentication

Many legitimate organizations have online services and request personal or financial information, including that of your kids. Where possible, implement ***multi-factor authentication (MFA)***, which is a means of verifying the user either through a text message or one-time only password.

Quick Guide

Keeping Your Kids Safe

continued

What are the risks?

Negative digital footprint

A "digital footprint" is your kids' online presence; who they appear to be and how people view them based on their actions using connected devices. The digital footprint they leave behind, however, requires careful consideration. There's always a chance that this footprint could be negative, and consist of things on the internet that you or your kids don't want up there, such as a silly photo, an inappropriate comment or a misinterpreted joke. Remember: even if deleted, everything you post can live on in the form of screenshots.

What can you do?

Privacy settings

Social media platforms have different privacy policies. Review them and update your kids' privacy settings regularly. Also, review what platforms they're on and if they're age-appropriate.

Take care in what you share

Encourage your kids to focus on creating a positive digital footprint. This includes being kind and respectful toward others at all times and keeping posts positive by highlighting special skills, achievements and helping others.

Defamation

What if your kids are impersonated by a fake or "spoof" account? Spoof accounts are easy to spot: they normally are new, have few (if any) followers or friends, and very few posts. The profile image will be the same as the true account or sourced from the true account's posts. Report spoof accounts to the platform, request they be deleted/removed and provide the link to your account as well as the link to the spoof account.

Online Scams

It's important for kids to be aware of the messages they're receiving on their devices, the real identity of the sender and the actions they're being asked to take.

1 **Spam:** Unwanted or uninvited communication, most commonly in the form of email or text messages.

2 **Phishing:** A fraudulent email or text message intended to steal private or personal information or install malware.

3 **Smishing:** When someone tries to trick you into giving them your private information via a text or SMS message.

Tips to avoid scams:

- **Avoid clicking on pop-ups, banners, online ads and special offers, and avoid participating in online quizzes and contests.**
- **Never respond to suspicious messages (spam, phishing or smishing) so scammers can't tell that the account or number is active, or get more information.**
- **Don't click on suspicious links or download suspicious attachments. Verify that they are actually from that person or organization in case their account has been compromised or spoofed.**
- **Beware of requests for personal information such as usernames, passwords or account numbers. Most legitimate organizations will not ask for this information.**

If your kids experience any of these scams or are unsure, they should show you or a trusted adult **immediately**.

- Try to figure out what has happened. Did they receive a suspicious message? Did they click any links or attachments? Did they provide any information? Take action by changing passwords and monitoring activity where necessary.
- If required, contact local law enforcement, who will be able to advise on the next steps or the appropriate persons to contact.
- Report spam to the Government of Canada's Fight Spam initiative **(www.fightspam.gc.ca)**.
- Report phishing and smishing to the Canadian Anti-Fraud Centre **(www.antifraudcentre-centreantifraude.ca)**.

Safe Communication Online

Your kids' time online often includes chatting with friends, sharing pictures or links, playing a game or watching videos. Some of these activities take place using social media platforms, mobile apps or a messaging system that can allow them to have conversations with people they may have never met in person or don't know very well. But, they don't know for sure who they're talking to.

Things to watch for:

1 | Exploiters

These are people who seek to take advantage of others online. They aren't always easy to spot because they often appear to be genuinely nice. However, they're trying to learn and use information about a person—like their interests or hobbies—as an opportunity to gain trust.

2 | Online lures

Exploiters typically use "lures" to trick kids into feeling comfortable. For example, they start by asking simple questions, then get more personal, or try to take advantage of kids' good nature and pretend they need help.

3 | Cyberstalking

Often taking place in the background and difficult to detect, cyberstalkers gather information and watch what your kids are doing. Their intentions may not always be clear, as these can range from curiosity to much more nefarious intent.

Your role as the parent or guardian:

Gut feelings

Encourage your kids to listen to their gut feelings! If something or someone feels suspicious or makes them uncomfortable, even if they don't understand why, they should listen to that feeling. Explain to kids that this feeling often happens when, deep down inside, they know something is wrong. Remind your kids: you wouldn't talk to a stranger on the street, so don't do it online.

"Stop, block, talk"

- **Stop** speaking with the exploiter right away.
- **Block** the exploiter, but don't delete the messages; instead, kids should share them with a parent, guardian or trusted adult.
- **Talk** to a parent, guardian or trusted adult immediately.

As the parent or guardian, if you see this going on and you are concerned for your kid's safety, contact your local law enforcement and they can advise you on next steps.

Safe Communication Online

continued

Your role as the parent or guardian:

When it's time for you to step in

It's recommended that parents or guardians regularly monitor younger kids' devices and online profiles. The age at which you stop monitoring will depend on family dynamics and each individual kid's maturity level. However, it's vital to always be on the lookout for suspicious messages, "followers" or "friends" who may be unknown to your kids in real life; and anyone who may have a negative influence on them.

Typically, kids who are being exploited or taken advantage of online will exhibit noticeable behavioural changes in their daily lives. Examples include but are not limited to: unexplained absences from school, attitude changes or shifts in their circle of friends and social activities.

If any of these changes appear to be the result of online activity, the first course of action is to sit down together, talk about and explain the risks, and collectively come up with solutions.

Cyberbullying

Cyberbullying involves the use of technology (social media, text messages, memes, websites, etc.) to make fun of and/or intimidate others. Unfortunately, what goes online, stays online forever. That's why it's so important to show your support and teach everyone the importance of taking a stand against cyberbullying.

We sat down with Matt Richardson, Director of Intelligence and Investigations, Anti-Human Trafficking Intelligence Initiative to discuss internet safety, cyber respect and building a positive online image. Here's what he had to say...

Expert Q&A | Responding to Cyberbullying

How would you define cyberbullying?

Cyberbullying is mean and malicious; it's intended to hurt; and there's typically a pattern of abuse that takes place over a period of time. Unfortunately, with cyberbullying, we can't leave it at the schoolyard or the workplace—it can follow us everywhere we go, making it relentless. Often there are a large number of people—the grey area, I call it—who are bystanders. They're aware of it, they're seeing what's happening and they're not standing up to the bullying. I see that as an opportunity to teach people how they can get involved in a positive, non-confrontational way by supporting the person who's being treated unkindly.

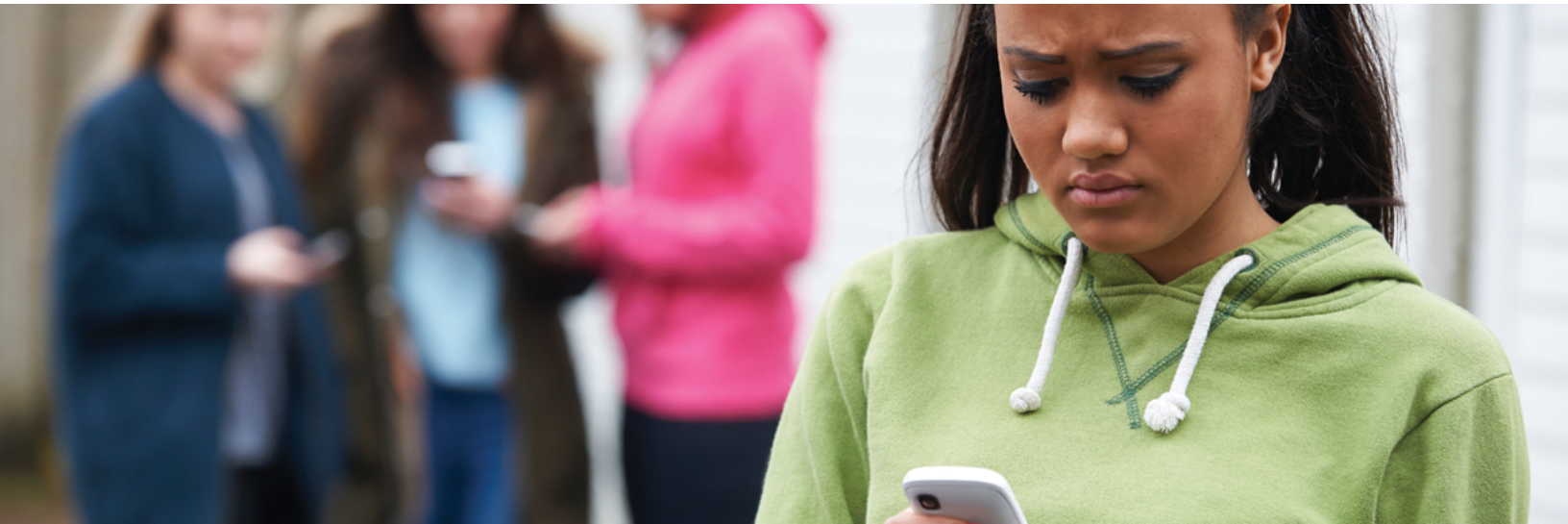
How can you tell if your child is being cyberbullied?

You might notice changes in their behaviour. If they want to stay home from school; if they're missing class and normally aren't like that; if they appear anxious, depressed or emotional; if, all of a sudden, they're not hanging out with their regular friends anymore. If you're present and engaged, you're going to notice in their behaviour that something's wrong.

When and how should a parent or guardian intervene?

There are different levels of bullying that require different approaches, but the situation can escalate quickly. First, I would give my son advice on good old-fashioned conflict resolution and I'll try to empower him with the skills to resolve it.

I wouldn't hesitate to get involved if my son was being relentlessly bullied and treated unkindly. How would I do that? First, say to your child: don't engage and don't start replying, because then it gets muddy. Second, take screenshots, because educators or police need evidence that something is happening.



Cyberbullying

continued

Step back, collect the evidence and try to keep them off social media until you can resolve it, because at this point, all it's doing is causing them agony and pain. Then I would go to the school principal, explain what's happening, including a basic idea of the timeline so I can articulate what's going on with accompanying screenshots. Then I would want to work with them on a plan of action.

The other thing I would do is a human thing. Try to give your child opportunities to forget about it and refocus. Do activities—something fun like taking them to a movie or bowling to can take their mind off of it. Try to get them away from the toxic people—and that's true for adults too, by the way.

What if your child is the bully?

Bullying is never acceptable and must be dealt with as soon as possible.

Start by calmly sitting down with your child and giving them the opportunity to tell you, in their own words, what happened. Explain that the actions were wrong and that bullying causes pain to others.

In many cases the punishment can range from being grounded, to being suspended from school, to criminal charges. Set expectations for their behaviour going forward.

If the bullying continues, seek additional support such as school personnel or counselling.

What advice would you give to a child who may be witnessing cyberbullying but doesn't know what to do?

Get involved with the person being bullied and show that you care. Be there to listen to them like a friend would do. Never confront the bully, don't get drawn in, but support the person and make them feel good—that's usually what people need most in those times. Be an upstander. Upstanders get involved in a positive way; bystanders pretend they're not seeing it.

One thing you can do is create a post saying something nice and tag your buddies that you know are kind. Create a whole conversation that you know will make that person's day.

Seeking Support

Kids dealing with cyberbullying can contact Kids Help Phone **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: **www.kidshelpphone.ca**

Keeping Devices Safe and Secure

To keep your kids safe, their devices also need to be kept safe. To learn more about how to recognize these risks and understand them, take a look at the following table.

1 | Securing devices

Your kids' devices—including laptops, tablets, cell phones and gaming systems—pose a risk to the security of your kids and your household. You should ensure that your kids' devices are safe and secure.

- Install and activate security software from reliable providers to help identify and block potential threats, while periodically checking that software is running correctly and up-to-date.
- Enable Auto-Lock/Screen Lock using a PIN, password or biometric signature (e.g., fingerprint).
- Ensure that kids use strong passwords or passphrases on all applications that have sensitive information. Never re-use passwords across multiple accounts.
- Block or disable applications that may be used for spying on your kids (camera, mic, location settings). Close the camera cover when not in use.
- Ensure that you allow operating system and software updates, as these often contain security patches that help keep you safe and secure.
- Disable autofill on passwords and other sensitive information (e.g., full name, SIN number, etc.).
- Set privacy settings to friends or followers only, and review settings periodically. Avoid having public profiles.
- Avoid connecting to public Wi-Fi—if you do, don't communicate sensitive information (e.g., online banking, personal information) while on it.
- Beyond the device, ensure that your home internet and Wi-Fi security are enabled; and that your kids' devices don't have permissions to access or change household systems.

Keeping Devices Safe and Secure

continued

2 | Disabling location sharing

Geolocation capabilities are included in most apps and services nowadays. However, this can also pose a risk as your kid's cellphone or other devices could be used to covertly locate and track them by bad actors.

- It's recommended to disable geolocation on camera, photos, video and other applications.
- If used for a particular activity that requires geolocation, disable geolocation when it's no longer needed.

NOTE: If you wish to install a safe tracking application on your kids' devices, then this is a discussion you should have with them, as they may have some concerns about their privacy.

---

3 | Browsing securely

Encouraging your kids to be critical thinkers and safe internet users will help protect them, their friends and their family from those who could do harm.

- Discuss safe searching practices, including words or phrases to avoid, and what to do if they stumble upon something that may be troubling.
- Emphasize critical thinking about online information and warn about false or malicious information.
- Where possible, avoid use of public Wi-Fi—not only can it be a source of cyber threats, but can be an access point into their devices by anyone who is on that network.
- Research and provide age-friendly search engines and filtering for age-appropriate content.

Keeping Devices Safe and Secure

continued

4 | Downloading safely

Downloading files and applications or clicking on links from untrusted sources can lead to problems, such as the installation of ***viruses***, ***malware***, and ***spyware***, providing access to cybercriminals.

- Ensure that you have security anti-virus software installed and activated on your home network and your kids' devices.
- Enable software and system updates from trusted providers, to keep your systems and kids' devices secure.
- Download only from trusted sources, websites and vendors. If unsure about whether the download is safe, conduct some research on the app provider and look for positive reviews or comments.

---

5 | Social media safety

Social media is a great way to keep connected to friends and family. It can also be a source of misinformation and a platform to support cybercriminal behaviour. Many social media platforms are used by cybercriminals to obtain information or coerce kids into doing things or providing information that could be harmful.

- Ensure that privacy settings are activated. Set accounts to 'private'.
- Encourage your kids to carefully consider what they post, who they communicate with and what they say, as these will become part of a permanent record that can follow them.

Keeping Devices Safe and Secure

continued

6 | Parental controls

With the rapid increase in the number of digital devices, games and applications, there's a wide variety of parental controls available.

- Consult the manufacturer's or provider's information, based on what you and your kids have agreed to.
- Balance the need for security and safety with age-appropriate responsibilities regarding downloading and viewing on internet-enabled devices.
- Most devices that have parental controls installed include remote monitoring. Consider discussing your concerns with your kids and decide what level of monitoring you're collectively comfortable with.

7 | Video game safety

Similarly, video game chat rooms or community groups can be fun and help players to better understand the world of the games. However, they can be a haven for people who do not have the best of intentions, especially in chatrooms and online gaming "communities". Also, some video games are built with enticements that require online or in-game purchases.

- Disable autosave for credit card information in the game or apps to avoid unexpected charges and reduce the potential for unauthorized access to your account.
- Monitor game use and encourage your kids to talk about their online gaming experiences.
- Ensure your kids are playing age-appropriate games.

Additional Resources

For more in-depth advice on cybersecurity, check out the Rogers Cybersecure Catalyst cybersecurity resources for youth in grades K-12: **www.cybersecurecatalyst.ca**

Others:

- Government of Canada – cybersecurity and protecting you and your family online: **www.getcybersafe.gc.ca**
- Government of Canada's Canadian Centre for Cyber Security – a unified source of expert advice, guidance, services and support on cybersecurity-related issues: **www.cyber.gc.ca**

Glossary

Trusted Adult: An adult that a child has a good relationship with and who has their best interests and safety in mind.

Passphrase: Passphrases often contain more characters than passwords do, but fewer components (for example, four words instead of 12 random characters).

Multi-factor Authentication (MFA): A security feature that verifies a user's identity by requiring two or more pieces of evidence ("factors") or credentials such as numerical codes, answers to unique security questions, etc.

Geolocation: The process of finding, determining and providing the exact location of a computer, networking device or equipment. It enables device location based on geographical coordinates and measurements.

Viruses: Code designed to secretly copy itself onto computer files or programs to destroy data and disrupt the functionality of computers and networks.

Malware: A virus secretly installed with the intent to steal private information, spy on a device or encrypt a device until the user pays money to the perpetrator.

Spyware: A type of malicious software (malware) that is installed on a device without a user's knowledge and steals private information and shares it with a third-party without consent.