Cybersecurity Checklist: Online Safety for Kids & Teens

Growing up online comes with opportunities and risks. Your kids are going to spend time online – it is expected and even essential in this tech era. Just as you take steps to protect them in the physical world, keeping them safe in the digital world takes similar vigilance and care. **Protecting your kids online starts with a conversation and this checklist will help your kids understand online safety and the roles we play in keeping our family safe.**

1. Share Less

Encourage your child to ask themselves if the information or photo they want to post is something they would give to a stranger. If the answer is no, don't post it.

What you can do:

- ❑ Personal Information: Talk to your kids about what information is considered private. Information that identifies you such as your full name, address, or phone number, should not be shared with anyone.
- ❑ Photos: Whether it's pictures of your home, family members, school, or vacation, sharing less is always better.
- ❑ Location: Disable geotags or location services in apps
- ❑ Email address: Your email address is personal — avoid posting it on public forums or entering it on sites you don't trust.

2. Be Smart with Passwords

We get it. Remembering new and unique passwords for every online account can be a pain. But so is getting hacked.

How to build a strong password:

- ❑ Use a different password for each of your important accounts.
- ❑ Use at least eight characters. The longer the better.
- ❑ Use combinations of letters (uppercase and lowercase), numbers, and symbols.
- ❑ Avoid common words like "password" or "user". Make your passwords memorable so you don't need to write them down, which would be risky.
- ❑ Immediately change your password if you think someone else knows it (besides a parent or guardian).
- ❑ Reset your passwords regularly.

3. Nothing is Free

What you can do:

- ❑ Keep the WIFI activity confined to your home. Public Wi-Fi is less secure than your private network.
- ❑ Delete any apps that you do not use.
- ❑ Skip the online quizzes and free apps. Often you 'pay' through sharing your personal information, online activities, location, contact list, text messages, and more.

4. Go Private

What you can do:

- ❑ Phone Settings: Review your child's phone privacy settings.
- ❑ Apps and Account: When signing up for a new account, your kids should not automatically accept the default settings. Assist them with creating new account, and its privacy settings.
- ❑ Social Media: Encourage your loved ones to go private and share less on their social media accounts. It makes it harder for strangers to connect with them online and view their online activity.

5. Fake Accounts and Scams

Many scams target children, from online shopping scams, fake contests and scholarships to online quizzes. With promises of deals, prizes and awards, these scams lure kids into clicking links and entering their personal details.

What you can do:

- ❑ Fake Accounts: Help them understand that people contacting them may not be who they say they are. Scammers creating a fake identity or account online to trick people into friending them or sharing their personal information.
- ❑ Fake websites: Scammers set up fake retailer websites that look like real online retail stores in these cases. The thing is, you won't receive the goods you paid for. Show them how to go directly to a trusted site.
- ❑ Fake Offers: If it sounds too good to be true it most likely is.
- ❑ Text Message or Phone Scams: If you don't recognize the number ignore it. Don't pick up, click or any links they text you and never give away personal information to someone you don't know.
- ❑ Email Scams: Don't open attachments or click on links if you don't know the source. If you receive an email with a suspicious attachment, simply ignore the email and delete it.

6. Security Settings

What you can do:

- ❑ Set up parental controls. The SafeSearch Filters feature on Google will block sites with explicit content.
- ❑ Set strong passwords and encourage your whole family to change their passwords regularly.
- ❑ Enable two-factor authentication, think of it as having more than one lock on your door.
- ❑ Don't install - or make sure you uninstall - those nosey apps or any apps you're no longer using.
- ❑ Turn on the "Find my Mobile" tool so you can locate missing devices and protect data.

7. Open Conversation

Protecting Your Kids Online Starts with a Conversation. The best way to protect your kids is to speak with them openly and regularly about cyber safety. Demonstrating that you trust their actions, while sharing advice for smart and safe online usage, can go hand in hand to create savvy and aware young people.

8. "I'm here for you."

No one likes to go through challenges alone and keeping safe online can be tricky. Emphasize to your child that should they encounter anything uncomfortable or upsetting online, that you're there for support. If they find themselves in a distressing situation (i.e., being cyberbullied or extorted), reassure them that they are not alone, and you'll get through this together.

This checklist is an important tool that can serve as an ongoing reference for you as you continue the conversation with your kids. While their online behaviours will evolve as they get older, this checklist can help remind you – and them – of the risks that exist on various platforms and devices. It's a good idea to print this out so you can check back regularly to stay on top of your children's online safety.

Report Fraud

If you believe your confidential information may have been stolen or obtained by a fraudulent party either online, by telephone or through any other means, call us immediately.

For general inquiries or comments regarding Privacy and Security, please also call us.
1-800-769-2511 (telephone banking)
1-800-769-2555 (online/mobile banking)
1-800-769-2512 (credit cards)
1-800-769-2535 (RBC Express online banking Client Support Centre)