Ontario

Cyber Security Tips for Parents and Students to Follow at Home

Overview

With the increased use of technology, the internet, and online learning from home, it is important for parents and students to take the right actions to help each other stay safe online. Fortunately, you don’t need to be a cyber security expert to better protect yourself online. Parents can follow the following security tips and share them with their children while at home.

Tip #1: Be alert and think before you click

Cybercriminals or individuals with malicious intent will use emails, texts or messages through social media, gaming and “fan” sites to impersonate a legitimate source or an individual you or your child may know to send attachments infected with malware (software intentionally designed to cause damage or harm) or links to fake websites that may look identical to a real/legitimate site, or offering “free stuff” that your child might be tempted to download.

- ✓ If you want to confirm an email, text or message is legitimate/valid, try to contact the sender (who may be an individual or organization) directly to enquire about the message received using their legitimate contact information and using a different method of communication (such as calling the sender to ask if they sent the message to you); You should not reply to the text message, call the number or click on any links in the message if you are unsure of its legitimacy;
- ✓ Never reveal personal or financial information in an email, text or message. Banks and medical offices will never ask for this information by email, text or message;
- ✓ Pay attention to website address you or your child visits, as harmful ones may use small differences in spelling or a different domain (e.g. .com versus .net); and
- ✓ Pay attention to who your child might be talking to on social media and gaming sites; and

Never click on links or attachments from emails, texts or messages you receive from unknown or suspicious sources.

Tip #2: Lock down user logins, and logout when not in use

Stealing user login information remains one of the preferred methods of cybercriminals.

- ✓ Create a different password for each user account;
- ✓ Create strong passwords that contains 15 or more characters using a mix of characters – including uppercase and lowercase letters, numbers, and symbols with random character placements;
- ✓ Update shorter passwords frequently;
- ✓ Do not write passwords down; Consider using a password manager application instead; If you have no other option but to write a password down, make sure you secure the paper in a locked cabinet or desk drawer);
- ✓ Do not share user logins and passwords with family members or others; and
- ✓ Where available (discuss with your school), set-up stronger security such as Additional Security Verification (ASV) –also known as multi-factor authentication which adds an extra layer of security to your user account; It requires both a password and another factor – like a code sent to your mobile device – during the login process.

Always logout from applications or devices when not in use and set auto logout where it’s available.

Tip #3: Secure your home network and only use secure home internet connections

Cybercriminals may obtain your personal or sensitive information by attacking unsecured Wi-Fi connections.

- ✓ Change the password of the administrator user account on the home internet router. Do not use the default password that came with the router.
- ✓ Ensure passwords on your home internet router and your home Wi-Fi network are strong, unique and updated regularly - please refer to tip #2 for tips related to making a strong password;
- ✓ If you are familiar with your router settings, ensure you use appropriate security settings; and
- ✓ Avoid using unsecured guest Wi-Fi networks (where no security key is required by the user).

Tip #4: Secure devices and keep software and apps up to date

Cybercriminals continually look to take advantage of software weaknesses on internet-connected devices.

- ✓ Install anti-virus/antimalware protection (also known as endpoint protection) on your devices from a known and trusted source;
- ✓ Keep software and applications (e.g. operating system, anti-virus/antimalware, internet browser, and productivity applications) on your devices (PCs, smartphones, laptops, tablets) up-to-date at all times (or in accordance with board processes for board-issued devices);
- ✓ Follow notifications to update software on your devices as they often help to repair important security weaknesses; and

If your school has established guidelines and processes for updating software, follow these practices for your school or board-issued devices.

Tip #5: Back up your data

Should your device be compromised by a virus/malware or be lost or stolen, having a backup/copy of your data and documents will allow you to recover your data/documents or continue work from another device.

When you backup your data, you create a copy of some or all the files on your device and store them in a separate location (e.g. external hard-drive, cloud drive, designated school network folder, if applicable). Some forms of backups can also store your device configurations to provide a restore point for the device. Backup and recovery software can automate the process by performing backups on a set schedule.

Tip #6: Follow school and board policies and procedures

When using devices provided by your school, or applications recommended by your school or school board:

Always follow policies, guidelines or best practices your school or school board may have communicated to you and your child.

Tip #7: Take immediate action if a security incident is suspected

If you suspect your personal/family device has been attacked, or your child’s personal device or school-issued device may have been compromised by a cyber security incident:

- ✓ Immediately disconnect the device from your home network and power it down before taking further action.

For compromises on school-issued devices, or any suspected school or board data privacy violation:

- ✓ Follow your school or board’s protocols and any reporting procedures in place.

Tip #8: Leverage security features of online tools and applications

When using online tools and applications these may come with default settings and/or additional optional features that can help to improve the security of your user account and the data you or your child enters the tool or application. If that is the case:

- ✓ Familiarize yourself with the security features that come with the tool or application as well as any recommended best practices that may have been communicated by the vendor for setting them up and using them effectively.
- ✓ For board or school recommended tools and applications, follow the guidelines, best practices or instructions your board or school may have communicated to you and your child.
- ✓ Activate and/or switch-on the additional security features in accordance with any board or school recommended best practices as well as any vendor instructions or recommended best practices.

Questions and Answers

1. What are some of the online security threats to students?

Children and teens can be targeted by the same kinds of security threats that affect adults. However, many children, especially younger ones, may not have the knowledge and experience to recognize cyber threats and take the right action. In addition, cybercriminals will find special ways to target children through “fan sites” or gaming and social media platforms using malicious links, pretending to be friends, offering “free stuff” that a child might be tempted to download that contains malware.

It is important for parents and students to be alert and be careful when using applications and devices. Following the above tips will help create a safer online experience.

2. What are strong passwords or passphrases?

The strength of a user login password directly affects how easy it is for another person to guess it or how long it takes for a malicious individual to crack it. Many successful attacks/breaches have been linked to weak passwords.

A strong password is one that usually contains 15 or more characters using a mix of characters – including uppercase and lowercase letters, numbers, and symbols with random character placements.

A strong passphrase is a password with multiple strange and uncommon words while still creating a phrase that gives you a mental picture you can remember.

3. Why should I regularly change my password?

Changing your password regularly reduces the danger of harm by cybercriminals.

- It prevents the use of saved passwords – if someone gains access to old and saved passwords (e.g. from an old device) it will no longer be useful.
- It limits access to your account by a keystroke logger or other eavesdropping method cybercriminals may use – if your password was already stolen. Regularly changing your

password makes it less likely that passwords used by cybercriminals in this way will be useful for any length of time.

Timeframes for changing passwords vary. You should follow any guidelines your school or school board may have set for this. You should also change passwords anytime you suspect you may have been targeted by a cyber attack. Changing your password regularly is one important action to reduce cyber security incidents.

4. Why would my child or I be at risk of cyber attack?

Cybercriminals do not pick particular people and are always looking for ways to attack systems, steal sensitive data (personal information and financial information) to make money and for other reasons. Online predators will specifically target children and may try to use social media, gaming platforms and other applications to communicate with children.

For cybercriminals, targeting people makes sense. In most cases, it is faster, easier and more profitable than targeting systems. Attackers take advantage of human nature with activities that trick people, such as creating a false sense of importance to do something or pretending to be trusted people.

Cybercriminals often use current events to create online scams. With global news sources currently focusing on the COVID-19 pandemic, there is an influx of COVID-19 related phishing and fraudulent emails, text messages, calls, and websites.

If there’s one thing that’s certain during a pandemic, it’s that cybercriminals will take advantage of the situation. Be extra vigilant when reviewing all emails and avoid clicking on suspicious links and attachments, especially when working from home. Home networks do not have the same level of security or monitoring as office networks.

Cybercriminals will try to make emails look legitimate. Double check before acting on anything! Just like any other type of potential phish, check if the email is from the correct email address or the source who it claims to be from (e.g., search for the email address online through a search engine such as Google).

5. How might my child become a target of an online predator?

When children go online, they have direct and immediate access to friends, family, and complete strangers, which can put them in danger. Children who meet and communicate with strangers online are easy prey for internet predators.

Online predators will specifically target children and may try to use social media, gaming platforms and other applications to communicate with children. The anonymity of online conversations could make children feel more comfortable and more likely to engage in risky behavior.

Online predators take a targeted, gradual approach and often devote considerable time and money through attention, affection, kindness, and even gifts to lure children. Parental oversight and supervision can help to reduce this danger.

6. Why should I consider using security features of online tools and applications?

Some online tools and applications may not come with the highest level of security features turned-on by default or there may be specific recommendations for how to use the tool or application in order to make it more secure for you and your child.

Not leveraging the additional optional security features that the tool or application provides or neglecting to use the tool or application in a secure manner could be putting you and your child at risk of a cyber security attack or data breach.

Familiarizing yourself with the security features provided and learning how to use the tool in the utmost secure manner could significantly reduce this risk for you and your child.

Helpful links to additional security resources

In addition to resources you may have received from your school or accessed online, below are other useful resources from the Federal Government's Get Cyber Safe website (www.getcybersafe.gc.ca) that provide additional details on some of the topics covered in this tip sheet.

- Make yourself more cyber secure (in five simple steps!) - (https://www.getcybersafe.gc.ca/cnt/blg/pst-20191015-1-en.aspx)
- Protect Your Devices – (https://www.getcybersafe.gc.ca/cnt/prtct-dvcs/index-en.aspx)
- Software updates: Why they matter for cyber security – (https://www.getcybersafe.gc.ca/cnt/blg/pst-20200115-2-en.aspx)
- Signs of a phishing campaign: How to keep yourself safe – (https://www.getcybersafe.gc.ca/cnt/blg/pst-20200311-1-en.aspx)
- The 7 Red Flags of Phishing – (https://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/phishing/ph2-en.aspx)
- Protect While You Connect — How to Stay Safe Online – (https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/prtc-cnct/index-en.aspx)
- 5 ways to protect your privacy on a new smart device – (https://www.getcybersafe.gc.ca/cnt/blg/pst-20181221-en.aspx)
- Here are three ways to keep mobile devices cyber secure – (https://www.getcybersafe.gc.ca/cnt/blg/pst-20191227-2-en.aspx)
    - You can also obtain regular updates on their Get Cyber Safe Blog (https://www.getcybersafe.gc.ca/cnt/blg/index-en.aspx).

The Canadian Anti-Fraud Centre (https://antifraudcentre-centreantifraude.ca/index-eng.htm) also provides information on fraud and identity theft. They provide information on past and current scams affecting Canadians, including information on the scams associated to COVID-19 (https://antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm).