SEPTEMBER

Cyber Hygiene:

Cyber awareness for back to school

Know your school's online code of conduct and technology acceptable use policies with school-provided devices or software.

Secure your personal devices

Use apps from official app stores to avoid installing potentially harmful apps.
Be cautious with browser extensions/add-ons – Some may appear harmless but could be collecting your data, scamming you, displaying unwanted advertisements and hijacking your browser. Only download from official marketplaces.
Set/update privacy settings – Use the most private options on your devices and apps. Periodically review privacy settings to make sure they have not changed due to a version update.
Set/update app permissions – Turn off unnecessary permissions. Pay special attention to apps that have access to your device location, contact list, camera, storage, and microphone – is the access needed?
Set device to auto-lock – Set a different PIN/password with biometrics on each device and have it auto-lock when the device is idle.
Only use safe WiFi hotspots and avoid using public WiFi without VPN.

Be Cyber Aware

Back to school can be an exciting time for everyone. Unfortunately, it's also an exciting time for cyber criminals as they seek to exploit kids unfamiliar with online risks. Consider the following discussion topics and encourage questions and dialogue:

- Cyber criminals – who they are and what they do.
- What do cyber criminals do with our personal information?
- How can kids stay safe?

Protection with Strong Passwords and Multi-Factor Authentication

Back to school is a good time to re-visit the question: what makes a powerful password? By following simple tips, you can help ensure your accounts and devices are safe.

- Longer is stronger. Use passwords that are 15 characters or more in length.
- UPPERCASE, lowercase, $ymbo!s and numb3rs – use a combination to ensure strong passwords.
- Use a passphrase to create meaningful and memorable passwords, for example, "MycuteGerbilWesley" or "BasketBallCamprOcks".

Secure your personal accounts

- **Make a list of all your user accounts** and delete ones you no longer need.
- **Consider separate accounts,** with one account limited for friends, family, and work, and other accounts for activities such as gaming and social media.
- **Adopt Multi-Factor Authentication (MFA)** if available on each user account to add an extra layer of security.
- **Set a strong password or passphrase** by following the advice above.
- **Set up unfamiliar activity alert notifications** on each user account to inform you of suspicious activities.
- **Do not** automatically sign in to apps with a social media account.
- **Do not** use the same user ID and password provided by your school on personal accounts.

K-12 Cyber Awareness Calendar

For more information: www.ecno.org/cyber-awareness

Ontario