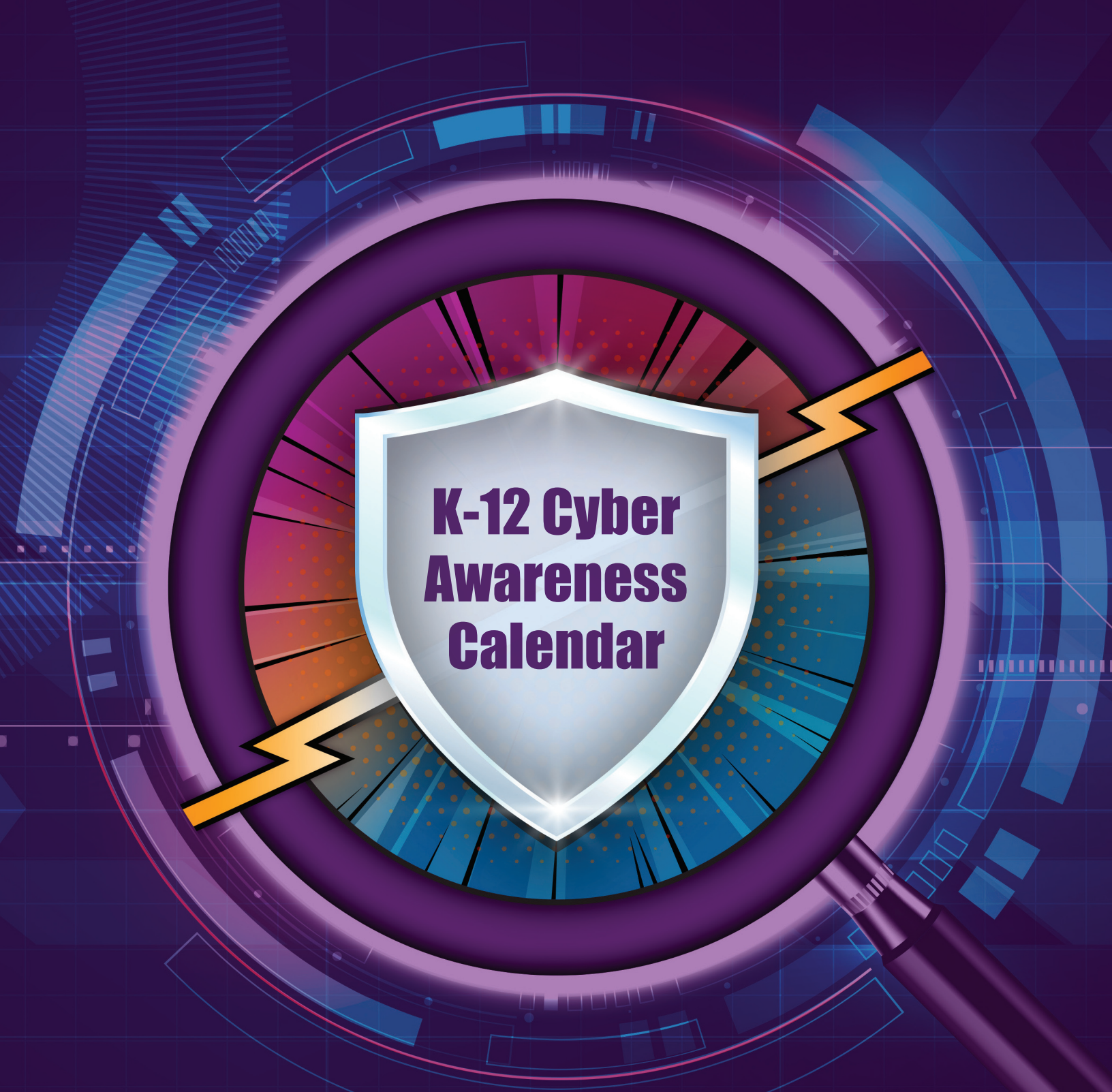


Encouraging Cyber Awareness throughout the year!

Ontario

Cyber Awareness Monthly Themes

September

Cyber Hygiene

Cyber awareness for a safe and organized back to school!

October

Cyber Awareness Month

Encourage safer and more secure practices across school communities surrounding the use of technology and the internet by promoting best practices in cyber safety, cyber security, and online privacy in K-12.

November

Be Kind Online

Learn about the ramifications of cyber bullying and the importance of being a respectful, kind internet user.

December

Cyber Scams and Phishing

All about malicious online activity used to trick people out of money and personal information.

January

Keep Your Information Private

The importance of managing and safeguarding your personal information online.

February

Online Grooming and Luring

Addressing the importance of staying vigilant and safe against digital predators who prey on children and youth for sexual exploitation.

March

Backup Your Data

Manage your digital footprint by maintaining a clean digital lifestyle through decluttering your digital space and backing up your data.

April

Safe Gaming and the Metaverse

Keep your online gaming fun by being aware of the dangers and threats that exist.

May

Digital Wellness

Encourage healthy habits in using technology and knowing your limits to maintain a healthy lifestyle.

June

Social Media

The importance of being proactive to protect yourself from the potential dangers of social media.

July

Digital Cleanup

The importance of deleting apps and accounts we no longer use to maintain a risk-free digital environment.

August

Connected Homes

Smart home technology provides benefits to everyday living, and it's important to be aware of the proper use of these technologies.

Ontario

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

NOVEMBER

Being Kind Online

Cyber Safety Top Three Tips:

1. Treat others online as you would want to be treated.
2. Stop and think before you post or send a message
3. Be fast to report.

Cyberbullying

Cyberbullying is online bullying to intimidate, hurt or humiliate someone. It can be very harmful because there is no safe zone. It can reach you anytime and anywhere, and can quickly be seen by a lot of people.

Cyberbullying examples:

- Sending mean or threatening emails or text/ instant messages.
- Sharing an embarrassing or a sexual image of someone.
- Pretending to be someone by using their name.
- Spreading hurtful gossip, secrets, rumours or lies.
- Ganging up on someone in a video game.

It can make you:

- Feel alone, sad, scared, frustrated or angry.
- Feel badly about yourself, your friendships, and your life.
- Want to avoid school, activities or anywhere else people may know you.

What can you do about it?

Be kind online:

- Don't send or post anything that might hurt someone else.
- Treat everyone you meet online with respect.

Be safe online:

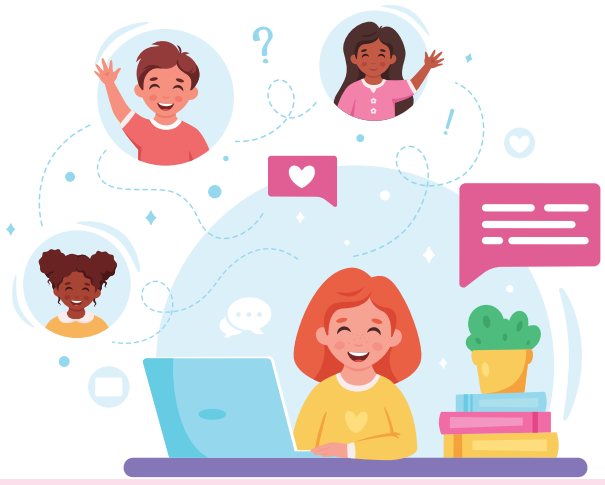
- Protect your privacy: use privacy settings on social media and don't share your personal information or passwords with anyone.
- Know who your friends are: be careful who you accept and restrict access for friends of friends and the public.
- Ask for help: if you made a mistake or are worried, feel threatened, or are being cyberbullied, talk to your parents or an adult you can trust.

If you are being cyberbullied:

- Don't reply with nasty messages.
- Block or break off contact with the person.
- Talk to your parents or a safe adult, your school, the site or app, or the police to get help.

If you see someone else being cyberbullied:

- Do not like or share messages – it can make things worse.
- If you know the bully and feel that it is safe to do so, tell them that cyberbullying is not okay.



K-12 Cyber Awareness Calendar

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

Ontario

DECEMBER

Cyber Scams and Phishing:

Don't be a victim!

A cyber scam is a criminal online activity designed to scam people out of money or personal information.

Most Common Types of Online Scams

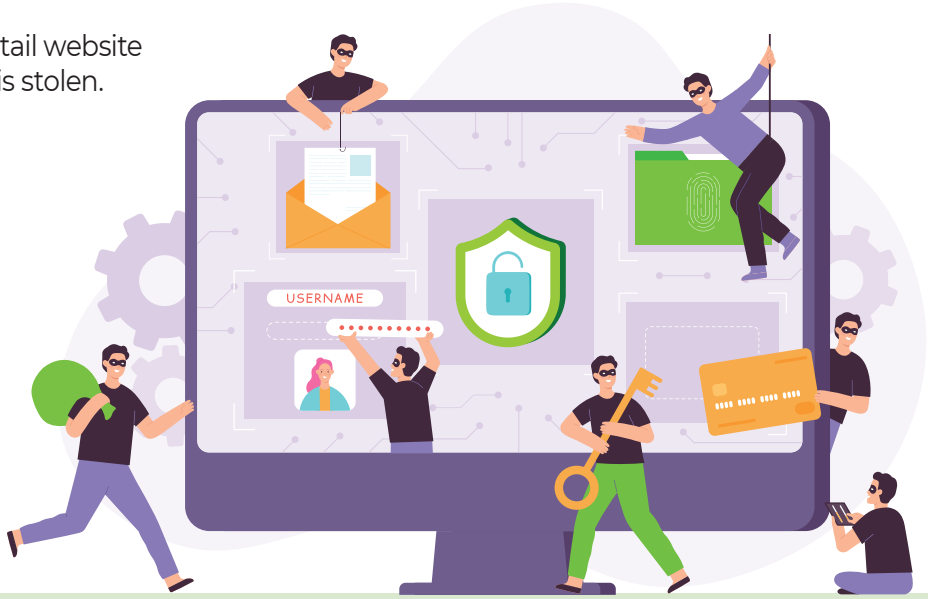
- **Phishing and Smishing** is a technique to "fish" for usernames, passwords, and other sensitive information, from a "sea" of users – through emails or text messages.
  - Phishing emails and smishing text messages may look like they're from someone or a company you know or trust.
  - These messages urge you to click a link, open an attachment, call a number or contact an email address.
  - The victim is then tricked into providing their personal information and credentials to other websites or services.
- **Fake apps are apps** created by cybercriminals to cause harm to users and their devices. They are designed to resemble legitimate apps but instead monitor your activity, install malware, or steal your personal information.
- **Websites that sell fake products.** These sites offer low-priced, high demand products that never arrive.
- **Formjacking** is when a legitimate retail website is hacked, and shopper information is stolen.

How to avoid scams:

- Do not open attachments, do not click links and do not respond to suspicious messages – ask questions, consult people you trust, or contact the sender using an alternative communication method.
- Avoid suspicious apps and deny permissions for something the app shouldn't be doing.
- Always use secure sites **(look for the S in https://)** when shopping or logging into your accounts online.
- Buy products from known marketers only.
- Do not post personal information on social media.

If you think you may be a victim of a scam:

- Stop all communication with the scammer.
- Seek help from an adult you trust.
- Report the scam to your local police.



K-12 Cyber Awareness Calendar

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

Ontario

JANUARY

Keep your Information Private

Manage your privacy and security settings on mobile devices!

Here are some tips:

- Limit personal information stored on devices.
- Use strong passwords and automatic lock features to prevent unauthorized access to mobile devices.
- Avoid public Wi-Fi hotspots for transactions that involve personal or financial information. Use a VPN or cellular data instead.
- Only download apps from authorized sites.
- Check permissions during the installation of an app. Understand what information the app can access on your device.
- Frequently check your "locations" settings to understand which apps are tracking you.

"To share or not to share – that is the question"

Planning and being on vacation and doing lots of fun activities can be exciting. However, wait until you return home to post any photos or videos. Announcing your trip on social media before leaving or while on vacation signals to thieves that you will not be home.

"TMI – Too much information"

It's important to understand what type of information can be shared online. it's okay to share your name, location and age with close friends. However, never post your address, full date of birth or geolocation publicly.

Protecting your reputation

Anything you post online or in a text message becomes part of your online identity. Here are some tips to help protect your reputation online:

- The internet never forgets. Nothing is temporary. It's important to remember this when chatting and posting online.
- Check your privacy settings often and ensure your profile is set to Private. This will ensure no one outside your profile can see your posts.
- Never post inappropriate or private pictures.
- Never respond to inappropriate requests.
- If something is bothering you, go offline, think about how you want to approach the situation and talk to a trusted adult.

K-12 Cyber Awareness Calendar

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

Ontario

FEBRUARY

Online Grooming and Luring

Online luring or grooming is when a person uses technology such as social media, gaming sites and/or chat rooms to convince children and youth to participate in sexual actions they do not want to do.

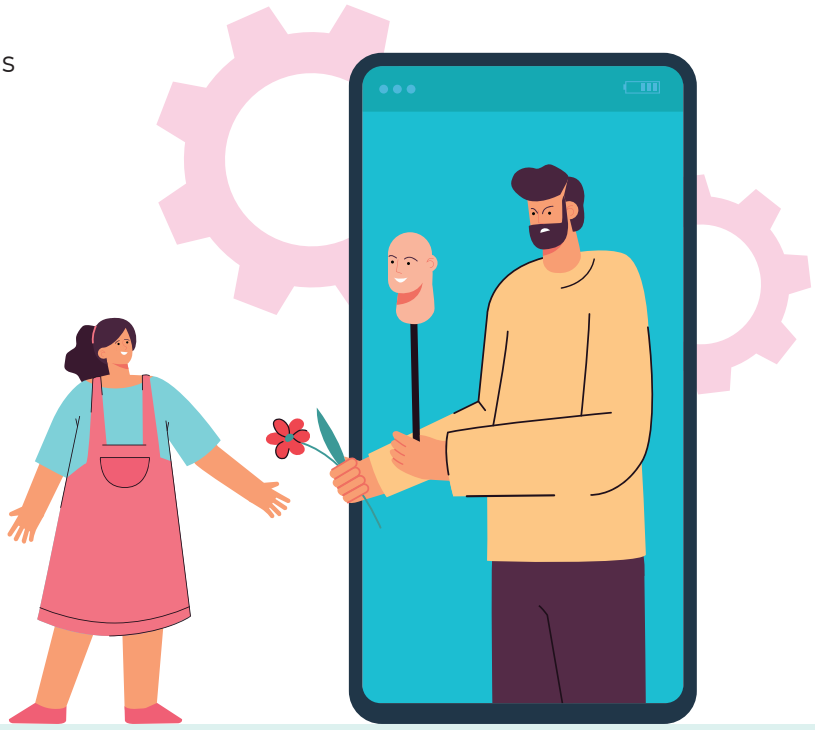
- Predators may **present themselves to you as a friend from school, a friend of a friend or someone you met** through extracurricular activities.
- **They may use flattery and compliments** to get you to warm up to them. Alternately, they may use intimidation, harassment and threats to control your interaction with them.
- They may **promise gifts** like a new phone, tablet, money, drugs or alcohol.
- They may **empathize with a vulnerability** you shared online, like a struggle you're having at home, to build trust and comfort.
- They may **exchange inappropriate pictures** with you as a way to convince you to send inappropriate pictures or videos in return. This may lead to **blackmail** like threatening to send inappropriate pictures to family and friends if you don't do what they say.

What to do if you think you're being lured

- Reach out to a trusted adult.
- If you need help right away, call **9-1-1.**
- To report sex trafficking and get help, call the Canadian Human Trafficking Hotline **1-833-900-1010** or visit **www.canadianhumantraffickinghotline.ca**

Online safety tips

- **Check friend requests and group invites before accepting them.** Check if you have friends in common and don't feel pressured to accept them.
- **Do not share any personal information** with anyone you have only interacted with online.
- **Avoid posting information** that may suggest problems or issues at home or school as the predator may use it to take advantage of your feelings and the situation.
- If someone online is offering you something **too good to be true** – like money or a new phone – it probably is. **Reach out to a trusted adult.**
- **Never share your location** or meet up with anyone you met online without first discussing it with a trusted adult.



K-12 Cyber Awareness Calendar

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

Ontario

MARCH

Backup your Data

Decluttering and backing up your data

Our digital life is consumed with so many activities – like browsing, chatting online and posting photos and videos. With various accounts, apps and devices within reach, our actions leave a digital footprint that makes it easier to be tracked by cyber criminals – putting our personal data at risk.

Apart from having numerous accounts and apps, we also produce a lot of data on our devices. This can cause our devices to slow down and increase our risk of losing important files along the way.

To ensure our data and devices are safe, it's important to maintain a clean digital lifestyle. This can be done by decluttering our digital space and backing up our data.

Cleanup to-do list

Here are some tips to keep your digital lifestyle clean:

- Remove applications that are not in use often.
- Delete your phone and browser history.
- Review your photos and videos, blurry, unnecessary and duplicates ones.
- Archive old emails.
- Unsubscribe from newsletter emails you don't read.

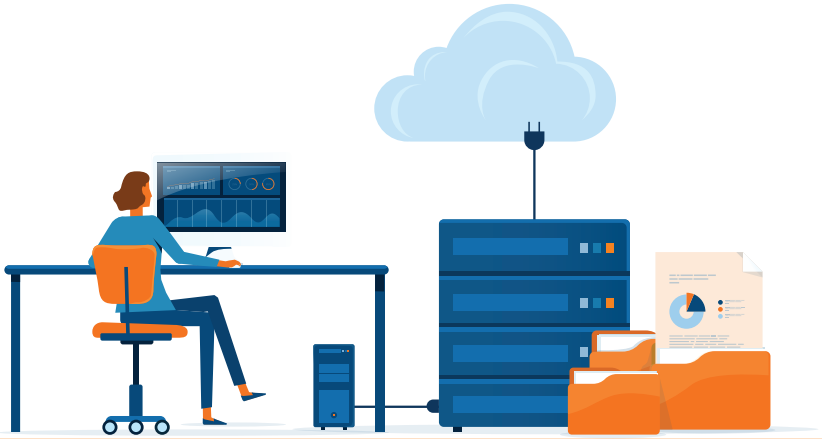
Backup data list

Prevent unnecessary data loss by doing the following:

- Review and sort your important files such as photos, videos, documents and emails routinely.
- Save and backup your files regularly.
- Consider backing up your data to an alternate location like an external hard drive or cloud storage.

The importance of cleaning and backing up your data

- **Peace of mind:** You don't have to worry about your electronic devices failing if your files are saved in backup storage.
- **Sufficient space:** Removing unnecessary files and apps from your devices will give you more space.
- **Secured data:** Less apps and accounts means less opportunity to access your data without authorization.
- **High performance devices:** Cleaning up data on your device will improve its performance and increase the battery life.
- **Less digital pollution:** Unnecessary files and data are digital trash. Digital trash creates digital pollution that continues to consume energy. Removing digital trash helps decrease electricity use.



K-12 Cyber Awareness Calendar

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

Ontario

APRIL

Safe Gaming and the Metaverse

Gaming safely online

Online gaming with friends can be so much fun! However, cyber criminals are using games to find ways to steal players' personal information. Here are some tips to game safely online:

- Do not use your own name, age, photo or any personally identifiable information for your avatar.
- Patch online games with the latest software updates and ensure anti-virus and anti-malware software is up-to-date.
- Choose games that are rated age appropriate – after all, the rating is there to protect you.
- Use a password or a passphrase to protect your accounts.
- Only use reputable sites to download games.

What is the metaverse?

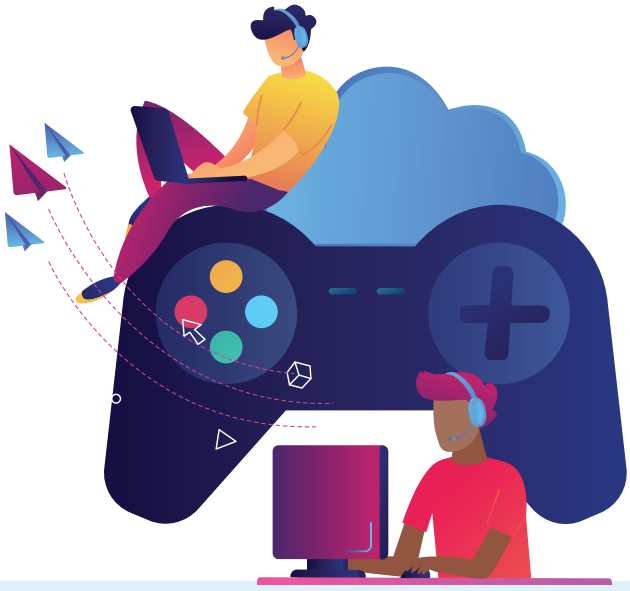
The metaverse is an online world – much like the real world – where people can interact as digital characters in 3D using a virtual reality headset. Apps can be downloaded for playing games, chatting or hanging out. It sounds fun and it is. But beware of dangers in the metaverse.

Dangers of the metaverse and how to protect yourself

- People aren't always who they say they are. An avatar can be anyone. Adults may pose as teens and lure you into private areas showing you graphic, inappropriate content. Approach others online with caution.
- The metaverse is not moderated. It is up to the user to report uncomfortable or inappropriate content, which might include cyberbullying, racism, and sexual harassment. Learn how to report such activity. Talk to a parent or a trusted adult about what to do if you get into an inappropriate or uncomfortable situation.

Tips for parents

- The metaverse is not intended for children under the age of 13 and there are no filters in place for age-appropriate content.
- VR applications and devices have limited parental controls. Take the time to learn about parental controls on VR/AR devices and application privacy controls.
- Access to the metaverse requires a VR/AR device and therefore there is no visibility – meaning others cannot see what is happening and cannot intervene to help. Encourage open dialogue and conversations about what is happening in the metaverse.



K-12 Cyber Awareness Calendar

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

Ontario

MAY

Digital Wellness

Using technology in a healthy way

Digital Wellness aims to promote healthy habits essential to using technology in ways to maintain a healthy lifestyle.

Ways to improve our digital wellness

- **Stay active** – Children and youth aged 5 to 17 years old should get 60 minutes of moderate-to-vigorous physical activity per day.
- **Limit recreational screen time** (not school related) to no more than 2 hours per day.
- **Get enough sleep** – Children ages 5–13 years old need 9–11 hours of sleep/night to feel refreshed while children 14–17 years old need 8-10 hours of sleep/night as part of a healthy lifestyle.
- **Build healthy relationships** – It's important that kids learn to engage with others and understand diverse perspectives and identities; empathize with others, listen and be respectful.
- **Discuss feelings about online activity** – Kids are encouraged to reach out to a parent or trusted adult to discuss online activity and let them know if something is upsetting them.

Prescription: Nature

It is commonly believed that nature has a positive effect on health and leads to improvements in overall mental health, self-esteem, ability to handle stress and resiliency.

Research has found that spending two hours or more in nature per week can improve overall health and well-being.

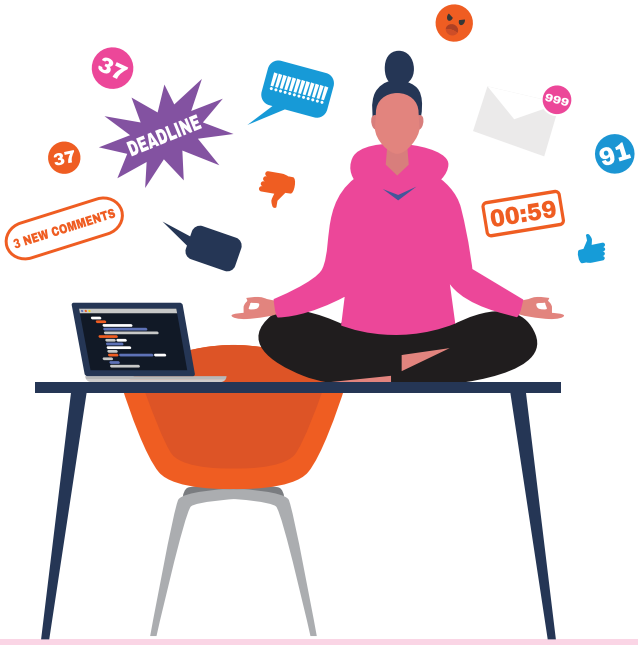
Here are some ways you can connect with nature:

- Unplug from technology and take a break from the screen.
- Go for a walk in a park or forest.
- Lay down in the grass and watch the clouds, listen to the sounds of nature.

Getting help

Kids Help Phone provides free, 24/7 confidential support for your mental health and well-being.

Help is available online by visiting **https://kidshelp-phone.ca/** or by calling **1-800-668-6868** OR texting **686868**



K-12 Cyber Awareness Calendar

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

Ontario

JUNE

Social Media

Going into the summer break, protect yourself and your information online

Summer is here and staying in touch with friends and family is easy using social media. It's important to be proactive and protect yourself from the harms of social media. Social media can be used in a safe way by following some simple tips.

Tips to using social media safely

- Ensure anything you post is private and can only been seen by your direct connections.
- Review your privacy settings frequently – especially after an application update.
- Think before you share online. Keep the following information private:
  - **Personal information** – Don't share your phone number, address, or full date of birth.
  - **Location** – Verify you're not sharing your location and remove geotags from older photos.
  - **Life news** – Post your vacation and events photos when you get back home.
  - **Financial information** – Don't post any bank or purchase information online.
  - **Other people's life updates** – Be careful with what you share about your friends and family. Always ask permission.

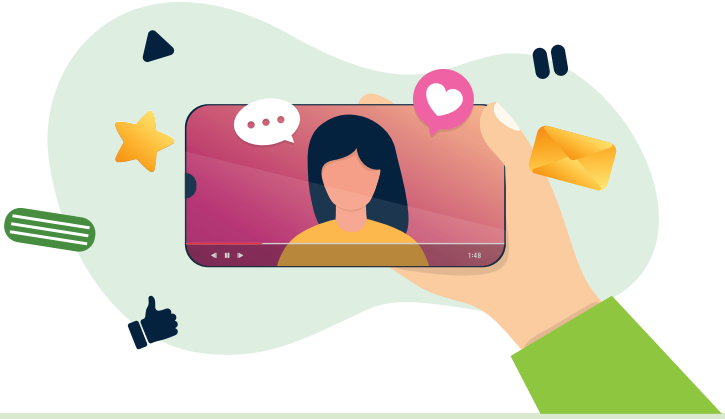
Overcoming FOMO and FOBO

Fear Of Missing Out (FOMO) is the anxious feeling of not knowing what your friends have been up to and the feeling you're not there to have fun with them.

Fear Of Being Offline (FOBO) is the anxious feeling of being disconnected with the online world.

To overcome this:

- Focus on meaningful and positive friendships, face-to-face interactions and actual experiences outside of social media – like going for a hike, riding a bike or going to the movie theatre.
- Know that your self-worth is not based on the number of likes you get online. Just because others get more likes does not mean they are more interesting than you.
- Remember photos and videos are only a small segment of someone else's life and are often highly edited.
- Follow people who inspire you, encourage positivity and happiness or those you could learn from! Learn to filter content that does not help your overall well-being.
- If you feel uneasy, talk to a parent, friend or trusted adult.



K-12 Cyber Awareness Calendar

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

Ontario

JULY

Summer Cleanup

Refreshing your digital space

Unused apps or programs

Take an inventory of the apps downloaded on your phone or computer. Are there any that have not been used for a while? If so, delete them to free up space and prevent old information from being shared. Some outdated apps may become unsecure so it's best to delete them to avoid any risk.

Accounts... going, going, gone

It's important to close or delete any accounts that are no longer in use. If not, there is greater risk to your digital privacy and security in the event of a data breach.

Accounts can be found by taking the following approach:

- Search for your name and email addresses.
- Consult your password manager for any unused accounts.
- Look through old emails.
- Check browser for old usernames and passwords.
- Check social media for old connected accounts.

Clear cache and cookies

Websites often store a large amount of user information in local storage and in the browser, making it a potential target for hackers. It's important to clear your cache and cookies frequently to increase your online privacy.

To protect yourself, you can:

- Customize your browser security settings to purge cookies when the browser is closed.
- Avoid saving credentials in the browser.
- Turn off autofill for any personal details.

E-Waste

Electronic waste (or e-waste for short) describes electronic devices that are no longer wanted. The good news is, these can be donated or recycled so they don't end up in the landfill.

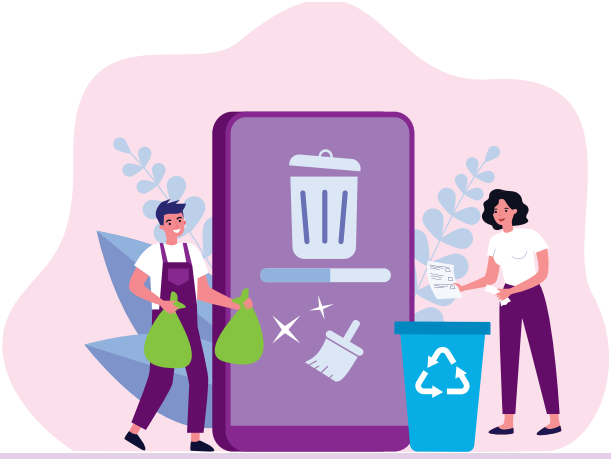
Types of e-waste that can be donated or recycled:

- Computers.
- Smartphones and tablets.
- Digital cameras and media players.
- External hardware – printers, monitors, external hard drives, USB sticks.
- Gaming consoles.

Before you donate or recycle your devices:

- Backup your information to another device or the cloud.
- Permanently erase data.
- Pull out hard drives and check that memory cards are removed.

To dispose of e-waste, search online for drop-off locations in your neighborhood.



K-12 Cyber Awareness Calendar

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

Ontario

AUGUST

Connected Homes

Staying secure at home

Things, things, so many things

Smart homes are increasingly common these days with various Internet-of-Things (IoT) devices – TVs, thermostats, light bulbs, kitchen appliances and even your outlets can be accessed using your smartphone.

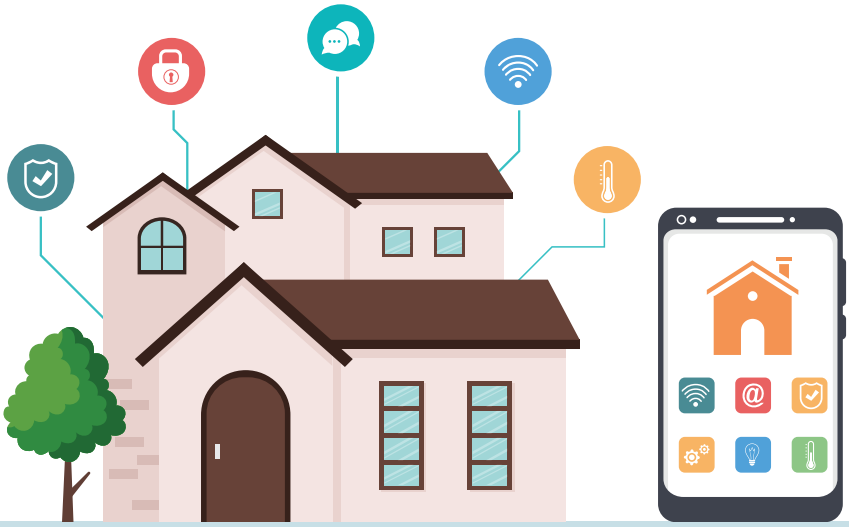
These amazing devices make it easier for people to be connected and in control of their homes. But having easy access to various devices also makes it easier for hackers to get your personal information. To stay connected and safe, here are a few things to remember.

How smart homes get hacked

- Unsecure Wi-Fi and routers – Smart homes can be hacked through unsecure Wi-Fi connections and unsecure routers.
- Devices may have minimal security – Many IoT devices are not designed for updates, making it easier for hackers to access them.
- Security features are not always enabled by default.

Best ways to secure your IoT devices and your smart homes

- **Connect IoT devices using an ethernet cable, if possible, instead of Wi-Fi** – If you are using Wi-Fi, ensure that it is password protected.
- **Change the default name and password on your Wi-Fi connection and router** – Default passwords are weak and easy to hack.
- **Think about what IoT devices you need in your home vs. what you want** – Consider the risk if any of your devices are hacked. What risk are you willing to accept?
- **Buy trustworthy brands and products** – Check product information and reviews online. Ensure devices have security features built in.
- **Use two-factor authentication, if available** – Using two-factor authentication enables additional security. In addition to a username and password, a second method of verification is required, like a code sent to your phone.
- **Keep your devices and apps up to date** – Install the latest updates on your devices and apps.



K-12 Cyber Awareness Calendar

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

Ontario