



2022-23 Cyber Awareness Calendar

September

Cyber Hygiene for Back to School

Sep 10 - World Suicide Prevention Day



October

K-12 Cyber Awareness Month Campaign



Oct 10 - World Mental Health Day

Oct 24-28 - Media Literacy Week

November

Being Kind Online



Nov 9 - Social Media Kindness Day

Nov 13-19 - International Fraud Awareness Week

Nov 20-26 - Bullying Awareness and Prevention Week

December

Cyber Scams and Phishing



January

Keep your Information Private!

Jan 23-27 - Data Privacy Week



February

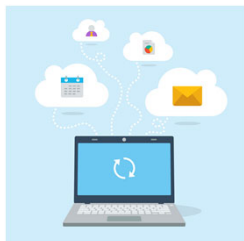
Online Grooming and Luring

Feb 14 - Safer Internet Day
Feb 22 - Human Trafficking Awareness Day



March

Backup your Data



Mar - Fraud Prevention Month

Mar 18 - Digital Cleanup Day

Mar 31 - World Backup Day

April

Safe Gaming and the Metaverse

Apr 12 - Identity Management Day



May

Digital Wellness

May 1-5 - Mental Health Week
May 5 - World Password Day



June

Social Media

Jun 5-11 - Environment Week
Jun 5 - Environment Day
Jun 16 - Stop Cyberbullying Day
Jun 30 - Social Media Day



July

Summer Cleanup



August

Connected Homes



September

Cyber Hygiene

Cyber awareness for back to school



Cyber Hygiene: Keeping your devices clean and safe

Laptops, phones and tablets all store lots of personal information about us - information cyber criminals find valuable. It's important we secure our devices correctly and apply simple cyber hygiene tips to avoid our personal information falling into the wrong hands.

Here are some ideas:

1. Install **anti-virus** and **anti-spyware** software - this is a great first level of defense.
2. Turn on **automatic updates** - software updates can be scheduled to automatically download and be installed overnight.
3. Check **privacy settings** often and minimize what can be viewed by others.
4. Ensure devices are **locked** by a **fingerprint, facial recognition, PIN or password**.
5. Ensure **web browser settings** are up-to-date with the latest version and clear your **cache** and **browsing history** often.



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.

Here are some topics to discuss with kids:

1. Cyber criminals - who they are and what they want.
2. What cyber criminals do with our personal information.
3. How kids can 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?**

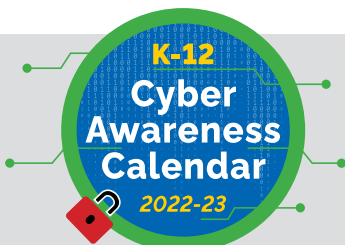
Here are some ideas:

1. **Longer is stronger** when it comes to passwords. Use passwords that are 15 characters or more in length.
2. **UPPERCASE, lowercase, \$ymbols and numb3rs** - use a combination to ensure strong passwords
3. Use a **passphrase** to create meaningful and memorable passwords. A passphrase is a string of words like "MycuteGerbilWesley" or "BasketBallCampOcks"

In addition to a password, **Multi-Factor Authentication (MFA)** can be enabled to help keep your accounts secure. **MFA** will ask you for an extra validation of who you are.

Types of validations can be:

- **Something you know** – like a password passphrase combination.
- **Something you have** – like your phone or a token.
- **Something that is part of you** – like your fingerprints.



Resources:

Cyber Security checklist

Securing your devices - Phones and tablets

Why multi-factor authentication is an essential part of cyber security

November

Being Kind Online

Bullying Awareness and Prevention Week Nov 20 to 26, 2022



Top three cyber safety 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 intended to **intimidate, hurt or humiliate** someone. It can be very harmful and have long-lasting consequences 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
- Revealing information considered to be personal, private, and sensitive without consent
- Pretending to be someone by using their name
- Spreading hurtful gossip, secrets, rumours or lies

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?

“Bee” 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



“Bee” kind online

- Don't send or post anything that might hurt someone
- Treat everyone you meet online with respect
- Compliment others in a meaningful way

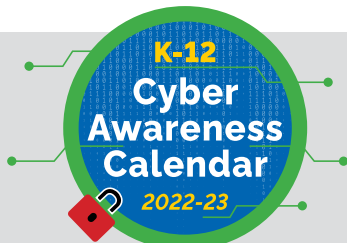
If you are being cyberbullied



- 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

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
- Talk to an adult you can trust so they can help you deal with it



Resources:

Bullying – we can all help stop it
What is cyberbullying?
From bystanders to upstanders



December

Cyber Scams and Phishing

Don't be a victim of cyber scams and phishing!



Today we are more connected than ever. Learn how to use technology wisely and be aware of online risks.

Most common types of cyber scams

Phishing and Smishing is a technique to “fish” or obtain 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 applications 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 shoppers get redirected to a fake payment page, where the scammer steals personal and credit card information.

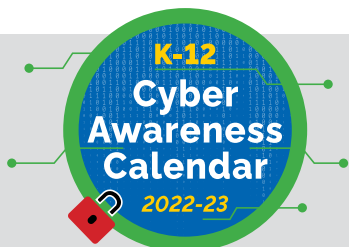
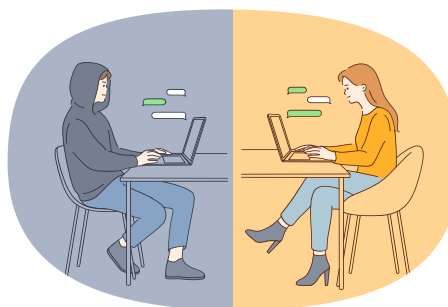
How to avoid scams

- 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



Resources:

Report a scam or fraud

Phishing: Don't get reeled in

Canadian Anti-Fraud Centre (1-888-495-8501)



January

Keep your Information Private!

Data Privacy Week Jan 23 to 27, 2023



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 app are tracking you.



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

Planning and being on vacation 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.

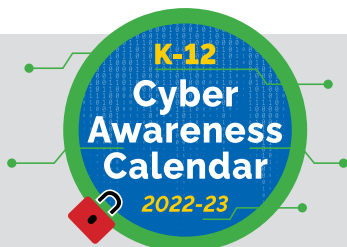
"TMI - Too much information"

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.



Resources:

Tips for protecting your personal information when downloading and using mobile apps

NeedHelpNow.ca - Helping teens stop the spread of sexual pictures or videos and providing support

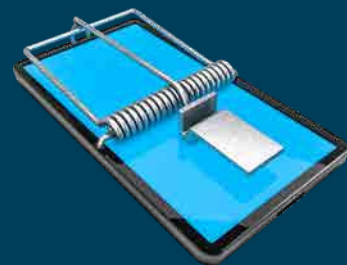
Share with Care - Protecting yourself and your online reputation



February

Online Grooming and Luring

Human Trafficking Awareness Day Feb 22, 2023



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.

What does luring and grooming look like?



- **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.

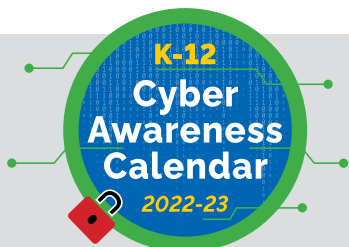


What to do if you think you're being lured

- 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

1. **Check friend requests** and **group invites** before accepting them. Check if you have friends in common and don't feel pressured to accept them.
2. Do not share any **personal information** with anyone you have only interacted with online.
3. 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 situation.
4. 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.
5. Never **share your location** or meet up with anyone you met online without first discussing it with a trusted adult.



Resources:

Signs that someone is being sex trafficked or sexually exploited
Online Luring - why teens are vulnerable and how to talk to youth about it
Online grooming: what it is and how to protect yourself

March

Backup your Data

World Backup Day March 18, 2023



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, erase 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:

1. Review and sort your important files such as photos, videos, documents and emails routinely
2. Save and backup your files regularly
3. 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.



Resources:

Does your data have a backup plan?
World Backup Day - Protect your data
How to back up your device: An introduction



April

Safe Gaming and the Metaverse

Identity Management Day April 12, 2023



Gaming safely online

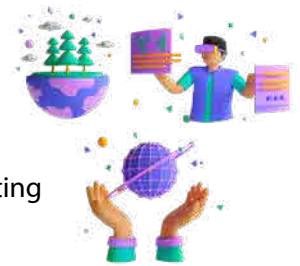
Online gaming with friends can be so much fun! However, cyber criminals are using games to find ways to steal players' personal information. Here are some tips to game safely online:

1. Do not use your own **name, age, photo** or any **personally identifiable information** for your **avatar**
2. Patch online games with the latest **software updates** and ensure anti-virus and anti-malware software is up-to-date
3. Choose games that are **rated age appropriate** - afterall, the rating is there to protect you
4. Use a **password** (or a passphrase) to protect your accounts
5. 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.



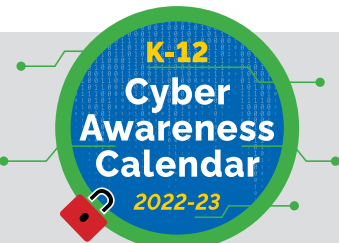
Dangers of the Metaverse and how to protect yourself

- **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.



Resources:

[Zoe & Molly Online - Resources for online gaming](#)

[Dangerous Reality: What parents need to know about the metaverse](#)

[Using virtual reality? Here are the cyber security risks you need to be aware of](#)

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

1. **Stay active** - Children and youth aged 5 to 17 years old should get 60 minutes of moderate-to-vigorous physical activity per day.
2. Limit recreational **screen time** (not school related) to no more than **2 hours** per day.
3. **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.
4. **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.
5. 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 ideas:

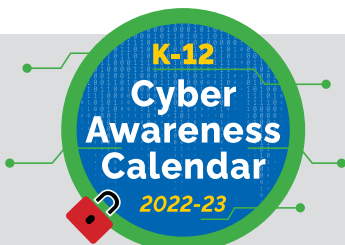
- **Unplug** from technology and take a break from the screen
- Go for a **walk** in a park or forest
- Lay down in the grass and watch the clouds, listen to the **sounds of nature**



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://kidshelpphone.ca/> or by calling 1-800-668-6868 OR texting 686868



Resources:

Four tips for managing your kids' screen time
Are Canadian children getting enough sleep?
A Prescription for Nature

June

Social Media

Social Media Day June 30, 2023



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

1. Ensure anything you post is **private** and can only be seen by your direct connections.
2. Review your **privacy settings** frequently - especially after an application update.
3. **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.



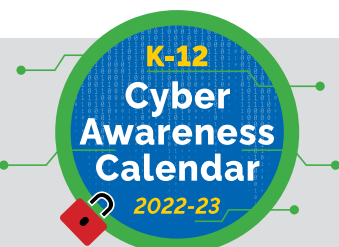
Overcoming FOMO and FOBO

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.



Resources:

Are your online friends who they say they are?
How to spot a cyber threat on social media
Guess What!?! quiz - Test your online (and offline) safety knowledge

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 insecure 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:

1. **Search** for your name and email addresses
2. Consult your **password manager** for any unused accounts
3. Look through **old emails**
4. Check **browser** for old usernames and passwords
5. 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.

Here are some ideas:

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

E-Waste

What is 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:

1. Backup your information to another device or the cloud.
2. Permanently erase data.
3. 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.

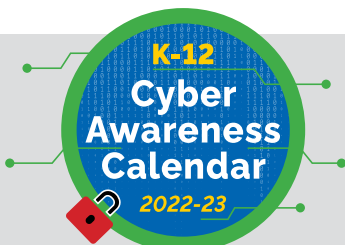


Resources:

justdelete.me - A directory of direct links to delete your account from web services

What you should know before recycling your device

Get Cyber Safe Agency - Workbook for kids





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.

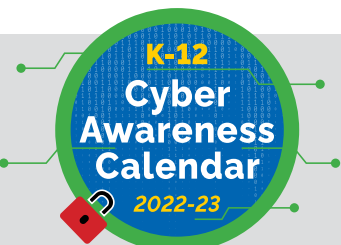
How smart homes get hacked

- **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.
- 
- An illustration of a hand holding a tablet. The tablet screen shows a user interface with a profile icon and a circular security overlay. Surrounding the tablet are several floating icons: a Wi-Fi symbol, a padlock, a smartphone, and a document with a checkmark, all in a light blue and purple color scheme.



Resources:

TVs and smart devices

Adjust privacy settings on your home digital assistants

Wearable devices and your privacy