K-12 Cyber Awareness Month 2021

Communications Products and Resources



Guide for School Boards on the K-12 Cyber Awareness Month 2021 campaign.

October 1st to 31st, 2021





Theme for 2021: **“Cyber awareness as self-care”**

**Weekly Themes for 2021:**

WEEK 1: Show your devices and accounts some love

WEEK 2: Pay attention to your home network and Wi-Fi connections

WEEK 3: Care for your personal information – it is valuable!



WEEK 4: Be mindful of your online presence and digital footprint



Online Safety

Online Privacy

Cyber Security

# K-12 Cyber Awareness Month 2021

The past 18+ months have shifted the way we rely on and interact with technology. In all areas of our lives, we have seen an unprecedented increase in the use of technology and the internet for staying connected, for recreation, for online learning, and more. Now more than ever, it is imperative that we learn to protect ourselves online.

October is internationally recognized as cyber security awareness month to help the public learn more about the importance of cyber security. **This is the second year we have created a Cyber Awareness Month (CAM) campaign tailored for K-12 needs, with a focus on cyber security, online safety, and online privacy.**

The campaign focuses on four weekly themes, based on the foundation that technology and the internet are part of our lives, and information and tips will be shared to help protect privacy and stay safer and more secure online.

Just as we lock our doors and secure our homes, visit the doctor to support our physical and emotional health and find peace in meditation to quiet our busy minds, caring for our online presence and digital footprint is just as important.

**“Cyber awareness as self-care!”** - Adopting safe, secure and healthy habits online is caring for your online presence and digital footprint, while helping to ensure you and your family are protected online.

# Weekly Themes and Content

##

## Week 1: Show your devices and accounts some love

## (October 4 to 8)

*Fortifying and locking down our devices and online accounts should always be a priority.*

Our devices and accounts are what we use to stay connected, to create and publish content, access online services, and play games. They are the doors to our online presence. We use our devices to authenticate who we are, communicate through email, texting, social media, and other tools, and we also use our devices to store personal information locally or in the cloud.

Many of us have multiple devices and accounts. Some are personal and some are for work, and some personal devices may be shared with other family members. Keeping track of it all can sometimes be challenging but it is important to do so.

This week take stock of your user accounts and devices and learn how to better protect them.

**Topics and tips for week 1 include:**

* Enabling the strongest authentication tools available on your devices and online accounts. (e.g. biometrics, multi-factor authentication, and strong passphrases or complex passwords).
* Keeping all software on your devices up to date. Setting your devices to automatically update.
* Installing anti-virus / antimalware software on your devices and keeping it up to date.
* Updating privacy and security settings on your devices and applications.
* Backing up your devices regularly.
* Setting age-appropriate parental controls on children’s devices and setting screen time and device boundaries.
* Knowing your school’s BYOD and acceptable use policies and following them.

##

## Week 2: Pay attention to your home network and Wi-Fi connections (October 11 to 15)

*Safe and secure Wi-Fi connections are just as important as having secure devices and online accounts.*

Nowadays most devices are connected to the internet through our home network, our school or office network, a data plan, or a public Wi-Fi hotspot. Many of the applications installed on our devices require an internet connection to access online services and function properly. Our devices will often look to connect to available Wi-Fi hotspots irrespective of whether that Wi-Fi connection is safe or not. It is up to the device user to ensure appropriate security and safety measures are taken when connecting to public Wi-Fi hotspots or deciding not to connect.

**Topics and tips for this week include:**

* Securing your home network and actively managing it. Considering updating your network router every 3-5 years to take advantage of improvements in security features.
* Taking stock of devices connected to your home network and monitoring for unusual activity.
* Setting up a guest network for your friends and visiting family members to separate their access and activity from all your home devices.
* Setting up a separate network for your smart devices, so if compromises occur, the threat remains isolated from your personal devices that contain personal and sensitive information.
* Kid-proofing your home Wi-Fi network to make it safer for children.
* Avoiding untrusted public Wi-Fi access; using a personal data plan or personal hotspot or using VPN when having to connect through an untrusted Wi-Fi hotspot.

##

## Week 3: Care for your personal information – it is valuable!

(October 18 to 22)

*It is more important than ever to protect our personal information.*

With personal devices, smart devices and the internet becoming a routine part of our lives, as we use them to work, learn, exercise, entertain ourselves and socialize, it is more important than ever to protect our personal information and teach our kids to develop habits that will make it part of their day-to-day routine. Like how children learn to be safe outdoors, children need to learn to be safe online.

**Topics and tips for week 3 include:**

* Protecting your personal information as it is valuable to you but also cybercriminals.
* Familiarising yourself with the terms and conditions of applications you use as some may be sharing your personal information with third-party organizations.
* Avoiding phishing attempts and online scams.
* Staying safe on social media and not oversharing personal information.
* Maintaining privacy while online and gaming.
* Reviewing and updating privacy settings and making it a habit.

##

## Week 4: Be mindful of your online presence and digital footprint

(October 25 to 29)

*It’s important to manage your online presence and digital footprint!*

This past year, kids have faced unique challenges, as many of their in-person activities have been replaced with an increased use of technology. This has resulted in an unprecedented increased online presence and digital footprint for most of us, adults, and kids alike.

Everyone should assume that what is shared online will remain online forever. Every action you take online, and information posted about you contributes to your “digital footprint” which can straddle our personal, student and professional lives. Improving our awareness of the traces of data we leave online and recognising how our individual digital footprints vary can help to improve the protection of our data online.

**Topics and tips for this week include:**

* Understanding what you post shapes your online reputation and becomes part of your digital footprint.
* Minimizing the risk of being a target of online harassment.
* Knowing that posts are not always private.
* Deleting accounts (and associated information) that you no longer need – old accounts and data can be risk.
* Navigating safely.

# Adopting or Tailoring the Campaign

The four-week K-12 Cyber Awareness Month (CAM) campaign is designed to be a comprehensive package, with resources relating to the theme of each week.

The K-12 CAM campaign and associated resources are offered as a ready for use package supported by communications toolkits in the hopes of minimizing the effort needed by boards to participate in the campaign.

Boards may still choose to tailor the K-12 CAM campaign to fit the boards’ unique needs. The campaign is intentionally modular and flexible. Some of the content developed by the campaign team is available in editable format to support this.

# Target Audience

The K-12 CAM campaign has resources for board staff, educators, students, and parents. Everyone can benefit from increased awareness of cyber/online risks and measures to protect themselves whether in a personal, educational, or professional setting.

Many of the topics and tips are universal and can apply to any setting. There may however be nuances in processes, procedures and policies from board to board, and school to school. Staff, educators, students and parents are encouraged to familiarize themselves with the specific processes, procedures and policies of their school board and school, and read any communication they may have received on the use of education technology.

# Communication and Engagement Strategies

Communicating the campaign information and resources out to your staff, educators, students (and their parents) is key to the success of running this campaign. School boards are encouraged to get their Communications Officer/Department involved and aware of the weekly themes and topics.

Strategize with your communications department on what channels you can use for this campaign. Examples of communication and engagement channels include:

* The school board’s website or intranet site
* The school board’s social media platforms
* Posters and print outs (this may not the best option given the pandemic situation)
* Emails to staff, teachers and students
* Classroom discussion topics
* Other school board communication tools

For greatest attention and impact, keep the communication succinct and catchy!

# Referenced Sources

The resources provided by this campaign are based on information from multiple reputable sources available in English and French. These include:

* Ontario Cyber Security Centre of Excellence - <https://www.ontario.ca/page/cyber-security-centre-excellence>
* Get Cyber Safe – Government of Canada - <https://www.getcybersafe.gc.ca/en/home>
* Office of Privacy Commissioner of Canada - <https://www.priv.gc.ca/en/>
* Information and Privacy Commissioner of Ontario - <https://www.ipc.on.ca/>
* RCMP - <https://www.rcmp-grc.gc.ca/>
* Canadian Centre for Child Protection - <https://www.protectchildren.ca/en/>
* MediaSmarts - <https://mediasmarts.ca/>
* Caring for Kids - <https://www.caringforkids.cps.ca/>
* Canadian Paediatric Society - <https://www.cps.ca/>
* Egale - <https://egale.ca/>
* White Ribbon - <https://www.whiteribbon.ca/>
* CAMH - <https://www.camh.ca/>
* Ophea - <https://www.ophea.net/>
* UNICEF - <https://www.unicef.org/>

# Other Awareness Campaigns

In addition to the themes and topics of the above K-12 CAM campaign, school boards also have the option of using campaigns and/or select resources from other reputable sources. Some of the themes and topics may be deemed to be more conducive to staff and may not include resources that cover all three pillars of cyber security, cyber safety, and online privacy.

The following are two awareness campaigns boards should be aware of.

## Ontario’s Cyber Security Division (CSD)

**Cyber Security Awareness Month 2021 Campaign (Launches October 1)**

This year marks the 10th annual Ontario Cyber Security Awareness Month campaign, featuring the theme ***The Anatomy of a Hack***. Each week in October, new material will be released for participants surrounding a cyber attack scenario. Participants will gain access to new content weekly which includes installations of a four-part graphic novel, educational videos, and quizzes. This content will teach participants how to protect themselves from modern-day cyber threats. All campaign content will be freely accessible through Ontario’s Cyber Security Awareness Month website.

If interested, visit Ontario’s CSD campaign website for more information: <https://cybersecurityontario.ca/mod/page/view.php?id=204&lang=en>.

Participants can also register to receive links to the weekly content that will be posted on the site, as well as upcoming content. To register, use the following link: <https://cybersecurityontario.ca/mod/page/view.php?id=171>.

This campaign is delivered with limited tailoring ability and the content will be released during each week in October.

## Get Cyber Safe, Government of Canada

[Get Cyber Safe](https://www.getcybersafe.gc.ca/en/secure-your-devices/gaming-systems) from the government of Canada has been providing awareness campaigns and resources for many years to inform Canadians about cyber security. Many of the resources they produce is leveraged in the K-12 CAM campaign.

Get Cyber Safe creates a Cyber Security Awareness Month campaign every year to help the public learn more about the importance of cyber security. This year the theme is ‘Life Happens Online’. For more information, consult the Get Cyber Safe website: <https://www.getcybersafe.gc.ca/en/cyber-security-awareness-month>.

For more information about the Get Cyber Safe weekly themes use the following link: <https://www.getcybersafe.gc.ca/en/csam-themes>.