K-12 Cyber Awareness Month 2022

Communication Products and Resources

Guide for School Boards on the K-12 Cyber Awareness Month (CAM) 2022 campaign

October 1st - 31st, 2022

Theme for 2022: **"Be a Cyberhero!"**

CYBER SECURITY

ONLINE SAFETY

ONLINE PRIVACY

Overview

For three years, ECNO (Educational Computing Network of Ontario), school boards and the Ministry of Education have partnered to develop a K-12 cyber awareness campaign for English- and French- language school boards in Ontario. The primary goal of the campaign is to help boards promote safer and more secure practices across their school communities when using digital technologies and the internet.

The purpose of this document is to provide school boards with an overview of the 2022 K-12 Cyber Awareness Month (CAM) campaign and associated resources. The 2022 October campaign is packaged for boards to use as-is or tailor it to meet specific board internal cyber awareness needs.

Each board can choose to direct their audience to the main ECNO campaign webpage or create their own branded landing page with links to campaign resources. Boards can also find information about other cyber awareness campaigns such as the Ontario Cyber Security Division's Cyber Security Awareness Month and the Get Cyber Safe Cyber Security Awareness Month, and may wish to leverage resources from those campaigns as well.

All boards are encouraged to review the myriad of cyber awareness resources available to them and determine what works best for their own cyber awareness campaign needs.

Introduction

During the past few years, we have seen the adoption of digital solutions and the internet at an unprecedented pace in every aspect of our lives - for work, education and staying connected with friends and loved ones. This has created a new normal for many where the use of digital technology is now more common practice in our day-to-day lives; this is true for all ages, young and old.

This quick and vast adoption of digital technology has increased cyber risks and online threats, as evidenced in the media and through various warnings issued by industry and government entities. Cybercriminals have taken advantage of this exponential increase in internet usage and continue to look for new ways to exploit users, irrespective of age.

We can all do our part to increase awareness related to cyber security, cyber safety, and online privacy, and in turn remediate cyber actions that can cause harm. Learning to be cyber safe and secure is essential to making our online experience more secure, fun, and rewarding.

By adopting safe and secure practices you are not only protecting yourself, but also reducing the likelihood of cyber-attacks against all members of the school community. Collectively, we can make our online and virtual lives safer for everyone by developing and maintaining personal safe online habits.

The **K-12 Cyber Awareness Month (CAM) campaign** has been developed to promote best practices in cyber safety, cyber security, and online privacy in the K-12 sector. The campaign is in its third year! It is an adaptation – tailored for the K-12 environment – of the internationally recognized October Cyber Security Awareness Month which is often mentioned in the media.

Theme

The theme of this year's K-12 CAM 2022 campaign is **"Be a Cyberhero!"**.

Staff, educators, school leaders and students of all ages can become cyberheroes by:

- Using the internet and digital technology for good, spreading positivity and respect
- Watching out for and reporting questionable activities such as phishing and scams – letting others know so they don't fall prey to the same phishing attempts and scams
- Standing up for themselves and others when hurtful or inappropriate online behaviour is noticed
- Keeping personal or sensitive information to themselves and continuously being thoughtful about which information to share online and with whom

- Acting as a school and board cyber ally – i.e., helping the board's IT and security team(s) by being the first line of defense in thwarting cyberattacks, being vigilant and doing their part in keeping board systems and information safe and secure
- Sharing and promoting what they learn about safe and secure practices with friends and loved ones

Each week in October promotes a specific topic.

- Week 1 focuses on social media, gaming, metaverse risks and best practices.
- Week 2 focuses on cyber scams and phishing risks, and what you can do to avoid being a victim.
- Week 3 is about good cyber hygiene for everyone to adopt and practice.
- Week 4 focuses on the importance of digital wellness, as we sometimes lose sight of the fact that we may be spending too much time online.

Below are details for each of the weeks.

Weekly Focus and Topics

WEEK 1: Social Media, Gaming and the Metaverse

Social media and online games are great ways to stay connected, interact and have fun with family and friends. It's essential to know how to do so safely – protecting your identity and personal information.

With the increase in popularity of the Metaverse (virtual and augmented reality), interactions with others are occurring in virtual 3D worlds via avatars and technologies such as virtual reality (VR) headsets and augmented reality apps. Some of these interactions can occur in unmoderated worlds increasing the risk of youth and children being exposed to inappropriate content and interactions.

Week 1 video: Learn to be a cyberhero by:

- knowing how to use social media safely
- learning to spot a cyber threat on social media
- staying cyber secure while playing video games
- recognizing the risks of the metaverse and how to reduce them

WEEK 2: Cyber Scams and Phishing

Cybercriminals are continuously finding new ways to scam/trick internet users of all ages. Their favorite techniques include phishing emails, phishing SMS or text messages (also known as smishing) and spoofing/using fake websites and phone numbers to try and trick us into divulging sensitive information such as our identity, personal information, account details and passwords.

Week2 video: Learn to be a cyberhero by:

- understanding what is phishing and recognizing the red flags to smash out scams before they strike
- understanding cyber villains' deceiving tactics and learning how to spot when you are being phished (quiz)
- recognizing fake emails
- knowing what to do with suspicious-looking messages
- teaching kids about phishing and how to avoid online scams

WEEK 3: Cyber Hygiene

Adopting thorough and accurate cyber hygiene habits can stop cyber villains in their tracks.

Fortunately for everyone, we can all train ourselves to think proactively about cyber security, online safety, and privacy by establishing solid cyber hygiene practices that become a routine as easily as brushing your teeth.

Week 3 video: Learn to be a cyberhero by

- protecting your accounts with multi-factor authentication and strong passwords or passphrases, and using a password manager to keep track of it all
- protecting your devices with antimalware and keeping software up to date
- adjusting privacy settings on devices and apps
- using secure Wi-Fi and VPN (virtual private networks)
- teaching kids about good cyber hygiene

WEEK 4: Digital Wellness

Even with cyber powers, cyberheroes need to take care of their personal well-being by knowing when to rest, pause and limit the use of digital technology and the internet. Learning how to moderate our use of digital technology is something we should all do.

Week 4 video: Learn to be a cyberhero by:

- knowing how healthy your relationship is with technology (digital wellness quiz)
- avoiding excessive use of digital technologies
- being mindful of the effects of social media use on us and others
- learning about the effects of sleep deprivation from using technology late into the night
- being kind online and blocking hurtful behaviour

Adopting or Tailoring the Campaign

School boards can choose to use the K-12 CAM campaign as defined; it is ready for use as a "campaign in a box". You can also choose to tailor it to align with your specific board needs and cyber awareness plans.

You may also want to supplement the campaign information with board-specific information such as policies, processes and procedures as a reminder to your K-12 community.

Communication and Engagement Strategies

The K-12 CAM campaign is for board staff, educators, students, and parents. Everyone can benefit from increased awareness of online risks, threats and measures to protect themselves.

Many of the topics and tips are universal to all audiences and can apply both in school and at home.

Communicating the campaign information and resources to your staff, educators, students, and parents is key to the success of achieving awareness outcomes of this campaign. School boards are encouraged to involve their communications officer/department and support their awareness of the campaign theme, the focus for each week, and associated topics.

Boards should strategize with their communications department on how the campaign will be communicated to the target audience and what channels will be used. Examples of communication and engagement channels include:

- promoting on the school and board's website, intranet or social media channels

- distributing posters and printouts
- sending emails to staff, teachers, and students
- involving Technology Enabled Learning and Teaching Contacts and promoting classroom discussions around the different topics
- involving parent councils
- posting on your board's Virtual Learning Environment

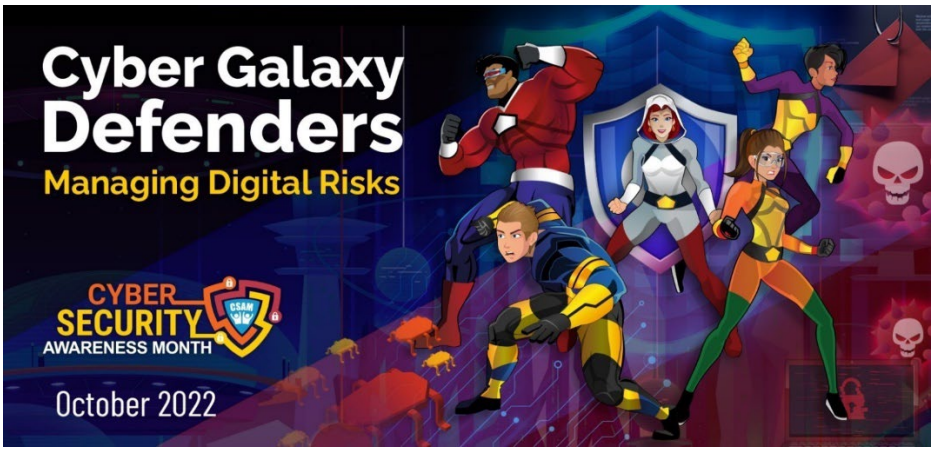
For greatest attention and impact, keep the communication succinct and catchy!

Other Awareness Campaigns

In addition to the K-12 CAM campaign described in this document, school boards may also wish to explore the following awareness campaigns from the Ontario Cyber Security Division (CSD) and Get Cyber Safe, a national public awareness campaign led by the Communications Security Establishment, created by the Government of Canada.

Ontario's Cyber Security Division (CSD)

The theme for this year's CSD campaign is ***Managing Digital Risks***. Throughout the month of October, CSD will share with the Broader Public Sector (BPS) – campaign information, interactive games and videos within the virtual cyber galaxy that present simulated cyber security threats, defenses and response actions. BPS organizations, including school boards, will be able to leverage the resources within their organization.



Follow this Link to obtain more information about the campaign or to register. The campaign offers three registration options.

Get Cyber Safe, Government of Canada

This year, Get Cyber Safe is focusing on ruining cyber criminals' days by teaching Canadians how to fight back against phishing scams. The theme 'Fight phishing: Ruin a cyber criminal's day' is covered over four weeks with the following weekly themes:

- week 1: You got phished
- week 2: Where, why and how it happens
- week 3: Prevention
- week 4: Putting it all together

For more information refer to the Get Cyber Safe Cyber Security Awareness Month webpage.