K-12 Cyber Awareness Month in a Box

Communications Products and Resources

Guide for School Boards as they prepare for their own K-12 Cyber Awareness Month campaign.

October 26 to November 20, 2020

Weekly Themes:

WEEK 1: Work, Teach and Learn from Anywhere

WEEK 2: Why Me?

WEEK 3: Think Before You Click, Post or Share

WEEK 4: Be Smart and Safe Online

Cyber Security

Online Safety

Online Privacy

K-12 Cyber Awareness Month 2020

A time to reflect on your online security, safety and privacy.

Cyber Security Awareness Month (CSAM) is an internationally recognized campaign traditionally held each October to inform people around the world of the importance of cyber security – this year being the 17th year. The K-12 Cyber Awareness Month (K-12 CAM) campaign is a modified version of the CSAM campaign tailored for the Ontario K-12 education environment.

The four-week K-12 CAM campaign is planned to run later, from October 26 to November 20, recognizing the new education realities and new ways of teaching, learning and connecting that students, parents and staff have had to embrace throughout September, October and beyond.

This year's campaign theme is "Work, Teach, Learn Remote, Secure and Safe" with an objective of helping everyone in K-12 education – teachers, staff, students and parents – be safer and more secure online. The campaign will provide resources to help everyone understand pertinent cyber threats and know a few simple steps to protect themselves, their workplace, learning space, and their devices.

The campaign is divided into weekly themes which highlight different aspects of cyber security, online privacy and online (cyber) safety, as all three areas are of equal importance to K-12. For each weekly theme, custom resources and links to resources from multiple reputable sources are provided.

Weekly Themes and Content

Week 1

October 26-30

WEEK 1: Work, Teach and Learn from Anywhere

Focus on cyber security and safeguarding your data, devices and systems.

With the COVID-19 pandemic, many have had to work, teach or learn remotely from home or other non-office or non-school locations. Although many school boards have returned to an on-site approach – working and teaching from school or board office locations – the risk of having to revert to a remote work and remote teaching arrangement remains, at least for the foreseeable future.

Although many elementary students are back in school for conventional in-person delivery, many parents have opted for remote learning. Secondary schools in some boards are following an adapted model that includes both in-class and remote learning.

Whether you are working or learning from a school, office, home or another remote location, we all have a responsibility to safeguard our devices – whether our own or board-issued; board systems or online education tools; and sensitive information whether our own, board business information or student personal information that teachers and board staff may collect or have access to.

This week we will look at the following:

- Using secure passwords and applying good user account practices
- Keeping your devices secure
- Securing your home network and the risks of using Wi-Fi from other remote locations
- Safely using videoconferencing tools for synchronous learning

Week 2

November 2-6

WEEK 2: Why Me?

Focus on understanding cyber threats and why cybercriminals or malicious individuals may be targeting you.

Why me? – is a common question you might ask yourself. Why would cyber criminals target me? The answer is that we either have valuable personal information or access to sensitive information that may be of interest to cyber criminals today or in the future, and that we may be used as leverage in a larger attack.

This week will focus on why teachers, board staff, parents and students need to be aware of online cyber threats and the motives of cyber criminals and individuals with malicious intent:

- Understanding cyber threats and how they work
- Ransomware and malware as a form of cyber threat
- Identity theft
- The long game for cybercriminals

Week 3

November 9-13

WEEK 3: Think Before You Click, Post or Share

Focus on being cautious online and protecting privacy and personal information.

This week, the campaign focuses on thinking before acting: clicking on a link in an email, text or website; posting information or photos on our social media accounts; and sharing sensitive information with colleagues, friends or outside agencies.

Malicious approaches such as phishing, smishing and fake websites or news will be covered this week. These techniques can be a tricky way for a cyber criminal to gain personal information and credentials. We need to think before we click on links that show up in our email and on messages in our phones.

- Don't be a victim of phishing, smishing or vishing
- Misinformation
- Think before you share or text

Week 4

November 16-20

WEEK 4: Be Smart and Safe Online

Focus on understanding the risks to student well-being.

Online safety is the theme for Week 4. It focuses on being aware of risks to different online activities, spotting threats and understanding how to stay safe while online. The Internet and the many different communication technologies such as laptops, smartphones, tablets and other smart devices, offer individuals of all age great opportunities for learning, exploration, fun and especially keeping in touch with friends and family during this pandemic. Unfortunately, these technologies can also present a host of concerns and worries ranging from accessing inappropriate content to being a victim of harassment or cybercrime.

This week will look at the following areas of risk:

- Online gaming

- Social media
- Sexual exploitation, sextortion and sexting
- Cyberbullying

This week also corresponds to Ontario's **"Bullying Awareness and Prevention Week"** which is an opportunity for the school community to raise awareness about bullying and cyberbullying and work together on prevention. We encourage you to learn more about this separate awareness campaign.

Tailoring the Campaign

The four-week K-12 Cyber Awareness Month campaign is designed to be a comprehensive package, with daily content relating to the K-12 theme of each week. The campaign can be used as is, or a school board could adapt the content to fit their individual needs and procedures.

Content will be provided in PDF and Microsoft Word (.docx) format so each board can download the content to use as-is or as a template for further tailoring.

Content will have a label indicating which content stream is covered (Cyber Security, Online Privacy or Online Safety). It also will have a label indicating to which audience the content relates (Staff and Administration, Educators or Parents/Students).

Feel free to download any content for use in your own campaign or link directly to this page.

Communication and Engagement Strategies

Communicating the campaign information and content out to your staff, teachers and students 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!

Campaign Content 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/