Mois de la cyber-sensibilisation de la maternelle à la 12e année 2022

Produits et ressources de communication

Guide de campagne 2022 du Mois de la cyber-sensibilisation de la maternelle à la 12e année à l'intention des conseils scolaires

Du 1er au 31 octobre 2022

Thème de 2022 : **« Deviens un cyberhéro! »**

CYBERSÉCURITÉ

PRUDENCE

CONFIDENTIALITÉ

Survol

Pendant les trois dernières années, le Réseau informatique éducationnel de l'Ontario (RIEO), les conseils scolaires et le ministère de l'Éducation ont travaillé ensemble à concevoir une campagne de cyber-sensibilisation de la maternelle à la 12e année. Cette campagne a pour but d'aider les conseils scolaires de langue anglaise et française à promouvoir des pratiques sécuritaires en ligne et avec les technologies numériques dans leurs communautés scolaires.

Le présent document donne aux conseils scolaires un aperçu de la campagne 2022 du Mois de la cyber-sensibilisation de la maternelle à la 12e année et des ressources offertes. La campagne, qui se déroulera en octobre 2022, a été conçue pour être menée telle quelle ou adaptée aux besoins précis du conseil scolaire.

Chaque conseil peut diriger son auditoire vers la page d'accueil de la campagne du RIEO ou créer sa propre page de renvoi, qui comporterait des liens vers les ressources pertinentes. En outre, les conseils peuvent s'inspirer d'autres campagnes du Mois de la sensibilisation à la cybersécurité – comme celles de la Division de la cybersécurité de l'Ontario et de Pensez cybersécurité – et tirer parti de leurs ressources.

Nous invitons tous les conseils scolaires à consulter la myriade de ressources à leur disposition et à déterminer celles qui sauront le mieux répondre aux besoins de leur campagne.

Introduction

Dans les dernières années, les solutions numériques et Internet ont pris une place prépondérante dans toutes les sphères de nos vies, que ce soit pour le travail, l'éducation ou simplement pour garder le contact avec nos proches. Le recours aux technologies numériques dans le quotidien est effectivement devenu la norme pour plusieurs, quel que soit l'âge.

Or, cette adhésion rapide et généralisée aux technologiques numériques augmente les cyberrisques et le nombre de menaces en ligne, comme le démontrent les médias et les nombreuses mises en garde d'organismes publics et privés. Les cybercriminels ont su profiter de cet engouement pour Internet et continuent de chercher de nouvelles façons d'exploiter les internautes de tous âges.

Or, nous avons toutes et tous la responsabilité partagée de sensibiliser les autres à la cybersécurité, à la sécurité en ligne et à la protection de la vie privée, et ainsi contrer les pratiques malveillantes. Il est essentiel de savoir se protéger pour naviguer en toute sécurité et ainsi vivre une expérience amusante et enrichissante.

L'adoption de pratiques sécuritaires vous permet non seulement de vous protéger, mais aussi de réduire les risques de cyberattaques pour l'ensemble des membres de la communauté scolaire. C'est ensemble, par l'acquisition de saines habitudes, que nous améliorerons la sécurité en ligne pour toutes et tous.

La **campagne du Mois de la cyber-sensibilisation de la maternelle à la 12e année (MCS M-12)** vise à promouvoir des pratiques exemplaires de cybersécurité, de sécurité en ligne et de protection de la vie privée dans le secteur de l'éducation, de la maternelle à la 12e année. Nous en sommes maintenant à la troisième campagne annuelle! Elle s'inspire du Mois de la sensibilisation à la cybersécurité – une campagne internationale très médiatisée qui se déroule chaque année en octobre –, mais a été adaptée pour mieux répondre aux besoins des milieux scolaires.

Thème

Le thème de la campagne 2022 du MCS M-12 est **« Deviens un cyberhéro! »**.

Voici ce que peuvent faire le personnel scolaire et les élèves de tous âges pour devenir des cyberhéros :

- Se servir d'Internet et des technologies numériques à bon escient, en lançant des messages positifs et respectueux.

- Être à l'affût des activités douteuses – comme l'hameçonnage et les arnaques – et les signaler, puis passer le mot pour éviter que d'autres se fassent prendre.
- Dénoncer les comportements blessants ou inappropriés en ligne à l'égard de soi ou des autres.
- Éviter de publier des renseignements personnels ou délicats, et toujours réfléchir avec qui les renseignements seront partagés tout en considérant les enjeux possibles de leur diffusion.
- Être une alliée ou un allié au sein des écoles et des conseils scolaires, et aider l'équipe des technologies de l'information et l'équipe de sécurité en étant au front pour prévenir les cyberattaques par une vigilance accrue et par la protection des systèmes et des données.
- Passer le mot sur les pratiques sécuritaires à ses amis et à ses proches.

Pour chaque semaine du mois d'octobre, il y aura un thème spécifique qui sera abordé :

- Semaine 1 : Risques et pratiques exemplaires liés aux médias sociaux, aux jeux vidéo et au métavers.
- Semaine 2 : Risques liés aux arnaques en ligne et à l'hameçonnage, et les mesures à prendre pour éviter d'en être victime.
- Semaine 3 : Bonnes pratiques de cyberhygiène.
- Semaine 4 : Importance du bien-être numérique, et la notion du temps accordé au numérique.

Voici le détail pour chaque semaine.

Sujets et questions prioritaires hebdomadaires

SEMAINE 1 : Médias sociaux, jeux vidéo et métavers

Les médias sociaux et les jeux vidéo en ligne sont d'excellentes façons de garder le contact, d'interagir et d'avoir du plaisir avec la famille et les amis. Mais il importe de savoir comment le faire en toute sécurité, c'est-à-dire protéger votre identité, vos renseignements et éviter des contenus et des interactions inappropriés.

Avec la popularité grandissante du métavers (réalité virtuelle et augmentée), les interactions se déplacent dans un monde virtuel en 3D au moyen d'avatars et de technologies comme les casques de réalité virtuelle (RV) et des applications de réalité augmentée. Or, ces univers virtuels ne sont pas tous sujets à la même surveillance, ce qui accroît les risques pour les jeunes et les enfants d'être exposés à du contenu et à des interactions inappropriées.

Vidéo de la semaine 1 : Apprendre à devenir un cyberhéro

- Savoir comment utiliser les réseaux sociaux de façon sécuritaire.
- Apprendre comment repérer une cybermenace sur les médias sociaux.
- Rester cybersécuritaire lorsqu'on joue à des jeux vidéo.
- Reconnaître les risques liés au métavers et les façons de les réduire.

SEMAINE 2 : Arnaques et hameçonnage

Les cybercriminels cherchent toujours de nouvelles façons d'arnaquer et de flouer les internautes de tous âges. Leurs modes de prédilection sont notamment l'hameçonnage par courriel, par messages texte ou messages de plateformes de médias sociaux (aussi connu comme du « smishing ») et d'autres arnaques comme l'utilisation d'un site Web ou de numéros de téléphone frauduleux pour inciter les victimes à divulguer des renseignements sensibles (identité, renseignements personnels, détails sur un compte, mots de passe, etc.).

Vidéo de la semaine 2 : Apprendre à devenir un cyberhéro

- Comprendre ce qu'est l'hameçonnage et savoir reconnaître les signes afin de freiner toute tentative d'arnaque.
- Comprendre les tactiques de tromperie des cybervilains et savoir comment repérer les tentatives d'hameçonnage (jeu-questionnaire).
- Reconnaître les faux courriels.
- Savoir quoi faire d'un message qui semble suspect.
- Apprendre aux enfants ce qu'est l'hameçonnage et la façon d'éviter la fraude en ligne.

SEMAINE 3 : Cyberhygiène

L'adoption de pratiques de cyberhygiène rigoureuses et efficaces peut contribuer à stopper net les cybervilains.

Heureusement, tout le monde peut adopter des pratiques saines en matière de cybersécurité, de sécurité en ligne et de protection de la vie privée avec une bonne cyberhygiène qui devient aussi routinier que se brosser les dents.

Vidéo de la semaine 3 : Apprendre à devenir un cyberhéro

- Protéger ses comptes avec l'authentification multifactorielle et des mots de passe et phrases de passe robustes, et en utilisant un gestionnaire de mots de passe pour ne pas perdre le fil.
- Protéger vos appareils avec un antimaliciel et en faisant les mises à jour logicielles.

- Ajuster les paramètres de confidentialité de ses appareils et applications.
- Utiliser un réseau Wi-Fi protégé et un RPV (réseau public virtuel).
- Parler aux enfants des principes de la cyberhygiène.

SEMAINE 4 : Bien-être numérique

Même avec des cyberpouvoirs, les cyberhéros doivent s'occuper de leur bien-être et savoir quand se reposer, prendre une pause et limiter l'utilisation des technologies numériques et d'Internet. Tout le monde devrait apprendre à faire preuve de modération.

Vidéo de la semaine 4 : Apprendre à devenir un cyberhéro

- Savoir si sa relation avec la technologie est saine (jeu-questionnaire sur le bien-être numérique).
- Éviter l'utilisation excessive des technologies numériques.
- Bien comprendre les effets du recours aux médias sociaux sur soi et autrui.
- Se renseigner sur les effets du manque de sommeil attribuable à l'utilisation des technologies jusqu'à tard dans la nuit.
- Faire preuve de bienveillance en ligne et bloquer les comportements blessants.

Utilisation et personnalisation du matériel

Comme la campagne de MCS M-12 a été conçue selon un principe « clé en main », les conseils scolaires peuvent utiliser les outils tels quels ou les adapter à leurs besoins et à leurs plans de cyber-sensibilisation.

Il est aussi possible pour un conseil scolaire d'ajouter des renseignements qui le concernent – politiques, processus et procédures –, en guise de rappel pour la communauté scolaire.

Stratégies de communication et de mobilisation

La campagne MSC M-12 s'adresse à l'ensemble des membres de la communauté scolaire, y compris les élèves, les parents, le personnel scolaire et les leaders des conseils scolaires. Une meilleure connaissance des risques et des menaces en ligne, et des mesures pour se protéger, profite à toutes et à tous.

En général, les points abordés sont universels et s'appliquent donc à n'importe quel auditoire, et à n'importe quel milieu (école ou maison).

Pour atteindre les objectifs de la campagne, il est primordial de transmettre l'information et les ressources aux membres du personnel scolaire ainsi qu'aux élèves et à leurs parents. Les

conseils scolaires sont invités à mettre à contribution leur service ou agente ou agent des communications pour voir à la diffusion du thème de la campagne, du sujet de la semaine et des questions connexes.

Les conseils scolaires devraient établir une stratégie avec leur service des communications pour bien communiquer les messages de la campagne au public cible et sélectionner les canaux à utiliser, par exemple :

- faire de la promotion sur le site Web, l'intranet ou les médias sociaux de l'école ou du conseil;
- distribuer des affiches et des feuillets;
- envoyer des courriels au personnel, aux membres du corps enseignant et aux élèves;
- mettre à contribution la personne-ressource en apprentissage et enseignement par la technologie et favoriser les discussions en classe sur les divers sujets;
- mettre à contribution les conseils de parents;
- faire des affichages sur l'environnement d'apprentissage virtuel du conseil.

Pour capter l'attention et maximiser les retombées, garder les messages courts et accrocheurs!

Autres campagnes

Outre la campagne du MCS M-12 décrite dans le présent document, il se peut que les conseils scolaires souhaitent explorer les campagnes de la Division de la cybersécurité de l'Ontario et de Pensez cybersécurité, une campagne nationale du Centre de la sécurité des télécommunications (gouvernement du Canada).

Division de la cybersécurité de l'Ontario

Le thème de la campagne de cette année est la ***Gestion des risques liés au numérique***. Tout au long du mois d'octobre, la Division de la cybersécurité publiera, à l'intention des membres du secteur parapublic, de l'information, des jeux interactifs et des vidéos sur le monde virtuel qui présentent des simulations de menace à la cybersécurité et des moyens de réagir et de se défendre. Les organismes du secteur parapublic, y compris les conseils scolaires, pourront ainsi tirer le maximum des ressources à leur disposition.

Suivez ce lien pour obtenir plus d'information ou pour s'y enregistrer. La campagne offre trois options d'inscription.

Pensez cybersécurité (gouvernement du Canada)

Cette année, Pensez cybersécurité a pour objectif de gâcher le plaisir des cybercriminels en montrant aux Canadiennes et aux Canadiens comment se défendre contre les arnaques par hameçonnage. Le thème « Combattez l'hameçonnage : Gâchez la journée d'un cybercriminel » est exploré pendant quatre semaines, à raison d'un sujet par semaine :

- Semaine 1 : Vous avez été hameçonné
- Semaine 2 : Où, pourquoi et comment cela se passe-t-il
- Semaine 3 : Prévention
- Semaine 4 : Mettre tout en commun et aider les autres

Pour en savoir plus, consulter la page sur le Mois de la sensibilisation à la cybersécurité de Pensez cybersécurité.