Trousse pour le Mois de la sensibilisation à la cybersécurité de la maternelle à la 12e année

Matériel de communication et ressources

Guide pour les conseils scolaires
qui préparent leur propre campagne du
Mois de la sensibilisation à la cybersécurité
de la maternelle à la 12e année.

Du 26 octobre au 20 novembre 2020

Thèmes hebdomadaires

SEMAINE 1 : Travailler, enseigner et apprendre de n'importe où

SEMAINE 2 : Pourquoi moi?

SEMAINE 3 : Réfléchir avant de cliquer, de publier ou de diffuser

SEMAINE 4 : Agir intelligemment et prudemment en ligne

Cybersécurité | Sécurité en ligne | Vie privée en ligne

Mois de la sensibilisation à la cybersécurité de la maternelle à la 12e année 2020

Un moment de réflexion sur votre sécurité et votre vie privée en ligne.

Le Mois de la sensibilisation à la cybersécurité (MSC) est une campagne reconnue à l'échelle internationale qui a habituellement lieu en octobre pour sensibiliser le monde entier à l'importance de la cybersécurité – cette année étant la 17e édition. La campagne du Mois de la sensibilisation à la cybersécurité de la maternelle à la 12e année (MSC M-12) est une version modifiée de la campagne du MSC adaptée au milieu éducationnel de la maternelle à la 12e année en Ontario.

La campagne de quatre semaines du MSC M-12 qui se déroulera plus tard, du 26 octobre au 20 novembre, reconnaît les nouvelles réalités de l'éducation et les nouvelles méthodes d'enseignement, d'apprentissage et de connexion que les élèves, les parents et le personnel ont dû adopter en septembre, en octobre et au-delà.

La campagne de cette année a pour thème « Travailler, enseigner et apprendre à distance en toute sécurité ». Son objectif est d'aider tous les acteurs du secteur de l'éducation, de la maternelle à la 12e année – enseignants, personnel, élèves et parents –, à être plus en sécurité en ligne. La campagne fournira des ressources pour aider chacun à comprendre les cybermenaces pertinentes et à connaître quelques mesures simples à appliquer pour se protéger, ainsi que son lieu de travail, son espace d'apprentissage et ses appareils.

La campagne est divisée en thèmes hebdomadaires qui mettent l'accent sur différents aspects de la cybersécurité, de la vie privée en ligne et de la sécurité en ligne, ces trois domaines étant d'égale importance pour tous, de la maternelle à la 12e année. Pour chaque thème hebdomadaire, des ressources adaptées et des liens à des ressources provenant de multiples sources fiables sont fournies.

Thèmes et contenus hebdomadaires

Semaine 1

Du 26 au 30 octobre

SEMAINE 1 : Travailler, enseigner et apprendre de n'importe où

Axée sur la cybersécurité et la protection de vos données, de vos appareils et de vos systèmes.

En raison de la pandémie de COVID-19, beaucoup ont dû travailler, enseigner ou apprendre à distance à partir de leur domicile ou d'autres lieux à l'extérieur des bureaux ou des écoles. Si de nombreux conseils scolaires sont revenus à une approche en présentiel – en travaillant et en enseignant depuis des écoles ou d'autres installations des conseils scolaires – le risque de devoir revenir à un système de travail et d'enseignement à distance est toujours présent, du moins dans un avenir prévisible.

Bien que de nombreux élèves de niveau élémentaire soient de retour à l'école pour un enseignement classique en présentiel, de nombreux parents ont opté pour l'enseignement à distance. Dans certains conseils scolaires, les écoles secondaires suivent un modèle adapté qui comprend à la fois l'apprentissage en classe et à distance.

Que nous travaillions ou apprenions à l'école, au bureau, à la maison ou ailleurs, à distance, nous avons tous la responsabilité de protéger nos appareils (les nôtres ou ceux fournis par les conseils scolaires), les systèmes des conseils scolaires ou les outils pédagogiques en ligne ainsi que les renseignements sensibles, qu'il s'agisse des nôtres, des renseignements professionnels de conseils scolaires ou des renseignements personnels d'élèves que le personnel enseignant et le personnel des conseils peuvent recueillir ou auxquels ils peuvent avoir accès.

Cette semaine, nous examinerons les éléments suivants :

- Utiliser des mots de passe sûrs et adopter de bonnes pratiques en matière de comptes d'utilisateur.
- Protéger vos appareils.
- Sécuriser votre réseau domestique et atténuer les risques liés à l'utilisation du Wi-Fi à partir d'autres lieux à distance.
- Utiliser en toute sécurité les outils de vidéoconférence pour l'apprentissage synchrone.

Semaine 2

Du 2 au 6 novembre

SEMAINE 2 : Pourquoi moi?

Axée sur la compréhension des cybermenaces et les raisons pour lesquelles des cybercriminels ou des individus malveillants peuvent vous cibler.

Pourquoi moi? – est une question courante que vous pourriez vous poser. Pourquoi les cybercriminels me cibleraient-ils? La réponse est que nous disposons de renseignements personnels précieux ou d'un accès à des renseignements sensibles qui peuvent intéresser les cybercriminels aujourd'hui ou plus tard, et que nous pouvons servir de levier dans une attaque plus importante.

Cette semaine sera axée sur les raisons pour lesquelles les enseignants, le personnel des conseils scolaires, les parents et les élèves doivent être conscients des cybermenaces en ligne, ainsi que des motivations des cybercriminels et des individus ayant des desseins criminels :

- comprendre les cybermenaces et leur fonctionnement;
- les rançongiciels et les maliciels comme forme de cybermenace;
- le vol d'identité;
- l'approche à long terme des cybercriminels.

Semaine 3

Du 9 au 13 novembre

SEMAINE 3 : Réfléchir avant de cliquer, de publier ou de diffuser

Surtout, faites preuve de prudence en ligne et protégez la vie privée et les renseignements personnels.

Cette semaine, la campagne porte essentiellement sur la réflexion avant l'action : cliquer sur un lien dans un courriel, un texte ou un site Web; publier des renseignements ou des photos sur nos comptes de médias sociaux; et échanger des renseignements sensibles avec des collègues, des amis ou des organismes extérieurs.

Les approches malveillantes telles que l'hameçonnage, l'hameçonnage par message texte et les faux sites Web ou les fausses nouvelles seront traités cette semaine. Ces techniques peuvent être une ruse efficace, de la part d'un cybercriminel, pour obtenir des renseignements personnels et des justificatifs d'identité. Il faut réfléchir avant de cliquer sur les liens qui apparaissent dans nos courriels et dans nos messages téléphoniques.

- Ne soyez pas victime d'hameçonnage, d'hameçonnage par message texte et d'hameçonnage téléphonique.
- La mésinformation.
- Réfléchissez avant de diffuser des renseignements ou d'envoyer un message texte.

Semaine 4

Du 16 au 20 novembre

SEMAINE 4 : Agir intelligemment et prudemment en ligne

Tâchez de comprendre les risques pour le bien-être des étudiants.

La sécurité en ligne est le thème de la quatrième semaine. Cette semaine se concentre sur la prise de conscience des risques liés aux différentes activités en ligne, la détection des cybermenaces et la compréhension des moyens d'assurer sa sécurité en ligne. L'Internet et les nombreuses technologies de communication telles que les ordinateurs portables, les téléphones intelligent, les tablettes et autres appareils intelligents, offrent aux individus de tout âge de grandes opportunités d'apprentissage, d'exploration, de plaisir et surtout de garder le contact avec leurs amis et leur famille pendant cette période de pandémie. Malheureusement, ces technologies peuvent également soulever une foule de préoccupations et d'inquiétudes de l'accès à un contenu inapproprié à être victime de harcèlement ou de cybercriminalité.

Cette semaine, nous nous pencherons sur les domaines de risque suivants :

- Jeux en ligne
- Médias sociaux
- Cyberintimidation
- Exploitation sexuelle, sextorsion et sextage

Cette semaine correspond également à la **« Semaine de la sensibilisation à l'intimidation et de la prévention »** de l'Ontario, une occasion pour la communauté scolaire de sensibiliser le public à l'intimidation et à la cyberintimidation ainsi que de travailler ensemble à la prévention. Nous vous encourageons à en découvrir plus sur cette campagne de sensibilisation distincte.

Adapter la campagne

La campagne de quatre semaines du Mois de la sensibilisation à la cybersécurité, de la maternelle à la 12^{e} année, est conçue comme un ensemble complet, dont le contenu quotidien est lié au thème hebdomadaire de la maternelle à la 12^{e} année. La campagne peut être utilisée telle quelle, ou un conseil scolaire peut en adapter le contenu à ses besoins et conformément à ses procédures.

Le contenu sera fourni en format PDF et Microsoft Word (.docx) afin que chaque conseil puisse télécharger le contenu pour l'utiliser tel quel ou comme modèle pour une adaptation ultérieure.

Le contenu aura une étiquette indiquant le volet de contenu traité (cybersécurité, vie privée en ligne ou sécurité en ligne). Il portera également une étiquette indiquant l'auditoire auquel se rapporte le contenu (personnel et administration, éducateurs ou parents et élèves).

N'hésitez pas à télécharger tout contenu pour l'utiliser dans votre propre campagne ou à créer un lien direct vers cette page.

Stratégie de communication et d'engagement

Le succès de cette campagne dépend d'une communication de renseignements sur la campagne et le partage de contenu avec votre personnel, les enseignants et les élèves. Les conseils scolaires sont encouragés d'impliquer leur chargée / département des communications et de les informer des thèmes et sujets hebdomadaires.

Établissez une stratégie avec votre département de communication sur les modes de communication à utiliser pour cette campagne. Voici des exemples de mode de communication et d'engagement:

- Le site Web ou le site intranet du conseil scolaire
- Les plateformes de médias sociaux du conseil scolaire
- Des affiches imprimées (ce n'est peut-être pas la meilleure option étant donné la situation de pandémie)
- Des courriels au personnel, aux enseignants et aux élèves
- Comme sujets de discussion en classe
- D'autres outils de communication du conseil scolaire

Pour une meilleure attention et un plus grand effet, gardez la communication succincte et facile à retenir!

Sources de contenu de la campagne

Les ressources fournies par cette campagne sont basées sur des renseignements de plusieurs provenances réputées et offertes en anglais et en français. Il s'agit entre autres des signes suivants :

- Centre d'excellence en cybersécurité de l'Ontario – https://www.ontario.ca/fr/page/centre-dexcellence-en-cybersecurite
- Pensez cybersécurité – Gouvernement du Canada – https://www.pensezcybersecurite.gc.ca/fr/homepage
- Commissariat à la protection de la vie privée du Canada – https://www.priv.gc.ca/fr/
- Commissaire à l'information et à la protection de la vie privée de l'Ontario – https://www.ipc.on.ca/?lang=fr
- Gendarmerie royale du Canada – https://www.rcmp-grc.gc.ca/fr
- Centre canadien de protection de l'enfance – https://www.protectchildren.ca/fr/
- HabiloMédias – https://habilomedias.ca/
- Soins de nos enfants – https://www.soinsdenosenfants.cps.ca/
- Société canadienne de pédiatrie – https://www.cps.ca/fr/
- Egale – https://egale.ca/
- Ruban blanc – https://www.whiteribbon.ca/francais.html
- CAMH – https://www.camh.ca/fr
- Ophea – https://www.ophea.net/fr
- UNICEF – https://www.unicef.org/