Mois de la cyber-sensibilisation de la maternelle à la 12e année – 2021

Produits et ressources de communication

Guide de campagne de 2021 pour le Mois de la cyber-sensibilisation M-12 à l'intention des conseils scolaires

Du 1er au 31 octobre 2021

Thème de 2021 : **« Se renseigner sur la sécurité en ligne, c'est prendre soin de soi! »**

Thèmes hebdomadaires de 2021

SEMAINE 1 : Prenez soin de vos appareils et de vos comptes

SEMAINE 2 : Faites attention à votre réseau domestique et aux connexions Wi-Fi

SEMAINE 3 : Prenez soin de vos renseignements personnels, car ils sont précieux!

SEMAINE 4 : Prenez conscience de votre présence en ligne et de votre empreinte numérique

Cybersécurité Prudence Confidentialité

Mois de la cyber-sensibilisation M-12 – 2021

Dans la dernière année et demie, nos façons d'utiliser la technologie et d'interagir avec elle ont été bouleversées. Dans toutes les sphères de la vie, nous avons assisté à une augmentation sans précédent de l'utilisation de la technologie et de l'Internet pour la communication, le loisir, l'apprentissage en ligne et d'autres motifs. Plus que jamais, il est impératif que nous apprenions à nous protéger en ligne.

Dans cette optique, le mois d'octobre a été déclaré mois international de la cyber-sensibilisation afin d'aider le public à en savoir plus sur l'importance de la cybersécurité. **Pour une deuxième année consécutive, nous avons créé une campagne pour le Mois de la cyber-sensibilisation (MCS) adaptée aux besoins de la maternelle à la 12e année (M-12), en mettant l'accent sur la cybersécurité, la prudence et la confidentialité en ligne.**

La campagne est axée sur quatre thèmes hebdomadaires, qui partent du principe que la technologie et l'Internet font partie intégrante de notre vie. Des renseignements et des conseils seront transmis pour vous aider à protéger votre vie privée en ligne et à naviguer de manière sécuritaire.

Déjà, nous verrouillons nos portes pour protéger nos maisons, nous nous rendons chez le médecin pour préserver notre santé physique et émotionnelle, et nous utilisons la méditation pour apaiser nos esprits occupés. De la même façon, il est important de prendre soin de notre présence en ligne et de notre empreinte numérique.

« Se renseigner sur la sécurité en ligne, c'est prendre soin de soi! » Adopter des habitudes sécuritaires, sures et saines sur le Web, c'est prendre soin de sa présence en ligne et de son empreinte numérique, tout en contribuant à assurer sa protection et celle de sa famille.

Thèmes hebdomadaires et contenu

Semaine 1 : Prenez soin de vos appareils et de vos comptes

(Du 4 au 8 octobre)

Renforcer et verrouiller nos appareils et nos comptes en ligne devrait toujours être une priorité.

Nos appareils électroniques et nos comptes nous servent à garder le contact, à créer et à publier du contenu, à profiter de services en ligne et à jouer à des jeux. Ce sont les portes de notre présence en ligne. Nous les utilisons pour valider notre identité, communiquer par courriel, par messagerie texte, sur les médias sociaux et à l'aide d'autres outils, et même pour stocker des renseignements personnels sur un support physique ou infonuagique.

Nous sommes nombreux à détenir plusieurs appareils et comptes. Certains sont destinés à un usage personnel, d'autres à un usage professionnel. Il arrive aussi qu'on partage des appareils avec d'autres membres de notre famille. Certes, il peut être difficile de suivre tout ce qui s'y passe, mais c'est important de le faire!

Cette semaine, faisons le point sur nos comptes d'utilisateur et nos appareils électroniques, et apprenons à mieux les protéger.

Sujets et conseils de la semaine 1

- Activer les plus puissants outils d'authentification offerts dans vos appareils et vos comptes en ligne (biométrie, authentification multifactorielle, phrases de passe robustes, mots de passe complexes…).
- Tenir à jour tous les logiciels de vos appareils. Configurer la mise à jour automatique.
- Installer un logiciel antivirus ou antimaliciel sur vos appareils et le tenir à jour.
- Modifier les paramètres de confidentialité et de sécurité de vos appareils et applications.
- Sauvegarder régulièrement les données de vos appareils.
- Établir un contrôle parental adapté à l'âge de vos enfants sur leurs appareils. Fixer des limites de temps d'écran et d'utilisation des appareils.
- Connaître et respecter la politique de votre école concernant les appareils personnels et leur utilisation acceptable.

Semaine 2 : Faites attention à votre réseau domestique et aux connexions Wi-Fi

(Du 11 au 15 octobre)

La sécurité des connexions Wi-Fi est tout aussi importante que celle des appareils et des comptes en ligne.

Aujourd'hui, la plupart de nos appareils électroniques sont connectés à Internet par l'intermédiaire d'un réseau domestique, du réseau de l'école ou du bureau, d'un forfait de données ou d'un point d'accès sans fil public. Bon nombre des applications installées sur nos appareils ont besoin d'une connexion Internet pour accéder à des services en ligne et pour fonctionner correctement. Souvent, les appareils tentent de se connecter aux points d'accès qui sont à leur portée – qu'ils soient sécuritaires ou non. C'est donc à l'utilisateur d'appliquer les mesures de sécurité nécessaires lors de la connexion à un point d'accès ou de décider de ne pas s'y connecter.

Sujets et conseils de la semaine 2

- Sécuriser votre réseau domestique et en assurer une gestion active. Songer à mettre à niveau votre routeur tous les trois à cinq ans pour profiter des améliorations apportées aux fonctions de sécurité.
- Vérifier quels appareils sont connectés à votre réseau domestique et surveiller toute activité inhabituelle.
- Configurer un réseau d'invité pour vos amis et parents en visite afin de séparer leur accès et leur activité de tous vos appareils domestiques.
- Mettre en place un réseau distinct pour vos appareils intelligents, de sorte qu'en cas de corruption, la menace soit isolée des appareils qui contiennent des renseignements personnels et confidentiels.
- Paramétrer votre réseau sans fil à la maison de façon à le rendre plus sécuritaire pour les enfants.
- Éviter les accès sans fil publics non sécuritaires. Utiliser plutôt un forfait de données personnel ou un point d'accès sans fil personnel, ou recourir à un réseau privé virtuel (RPV) si vous devez passer par un point d'accès non sécuritaire.

Semaine 3 : Prenez soin de vos renseignements personnels, car ils sont précieux!

(Du 18 au 22 octobre)

Il est plus que jamais important de protéger nos renseignements personnels.

Les appareils personnels, les appareils intelligents et l'Internet font désormais partie intégrante de nos vies : nous les utilisons pour travailler, apprendre, bouger, nous divertir, communiquer, etc. Il est donc plus important que jamais de protéger nos renseignements personnels et d'apprendre à nos enfants à en faire une habitude au quotidien. Tout comme les enfants apprennent à être prudents à l'extérieur, ils doivent apprendre à être prudents en ligne.

Sujets et conseils de la semaine 3

- Protéger vos renseignements personnels, car ils ont de la valeur non seulement pour vous, mais aussi pour les cybercriminels.
- Vous familiariser avec les conditions d'utilisation de vos applications, car certaines peuvent transmettre vos renseignements personnels à d'autres entreprises.
- Éviter les tentatives d'hameçonnage et les fraudes en ligne.
- Faire preuve de prudence sur les médias sociaux en évitant de diffuser trop de renseignements à votre sujet.
- Protéger votre vie privée lorsque vous naviguez sur le Web et jouez à des jeux vidéo.
- Revoir et modifier vos paramètres de confidentialité, et en faire une habitude.

Semaine 4 : Prenez conscience de votre présence en ligne et de votre empreinte numérique

(Du 25 au 29 octobre)

Il est important de vous occuper de votre présence en ligne et de votre empreinte numérique!

L'année dernière, les enfants ont dû relever des défis uniques, car nombre de leurs activités en personne ont été remplacées par une utilisation accrue de la technologie. Ainsi, ils ont vu leur présence en ligne et leur empreinte numérique s'amplifier comme jamais auparavant – à l'instar des adultes.

Nous devrions toujours tenir pour acquis que ce qui se retrouve en ligne y restera pour toujours. Chaque geste posé en ligne et chaque information publiée à votre sujet alimentent votre « empreinte numérique », qui peut englober diverses sphères de votre vie : personnelle, étudiante et professionnelle. En prenant conscience des traces que vous laissez en ligne et en sachant que l'empreinte numérique peut varier d'une personne à l'autre, vous pourrez mieux protéger vos données.

Sujets et conseils de la semaine 4

- Prendre conscience que ce que vous publiez façonne votre réputation en ligne et fait partie de votre empreinte numérique.
- Atténuer le risque d'être la cible de harcèlement en ligne.
- Savoir que les publications ne sont pas toujours privées.
- Supprimer les comptes (et les données qui y sont associées) quand ils ne sont plus nécessaires, car ils peuvent constituer un risque.
- Naviguer en toute sécurité.

Utilisation et personnalisation du matériel

Le Mois de la cyber-sensibilisation de la maternelle à la 12^{e} année se veut une campagne complète, avec une thématique et des ressources différentes pour chacune des quatre semaines.

La campagne, ses ressources et les outils de communication sont fournis clé en main afin de réduire le plus possible la charge de travail des conseils scolaires participants.

Les conseils peuvent cependant décider d'adapter la campagne à leurs besoins uniques. Les ressources, modulaires et modulables, ont été pensées à cette fin; seront d'ailleurs disponibles les versions modifiables de certains des documents préparés par l'équipe de la campagne.

Public cible

Dans le cadre de la campagne MSC M-12, des ressources sont mises à la disposition du personnel des conseils scolaires, des éducatrices et éducateurs, des élèves et des parents. Tout

le monde peut enrichir ses connaissances sur les cyberrisques et les moyens de se protéger, que ce soit dans sa vie personnelle, à l'école ou au travail.

Une bonne partie des points abordés est universelle et s'applique donc à n'importe quel contexte. Cela dit, les processus, procédures et politiques peuvent différer légèrement d'un conseil à l'autre ou d'une école à l'autre. Le personnel, les éducatrices et éducateurs, les élèves et les parents sont invités à se familiariser avec ce qui concerne leur conseil scolaire et leur école, et à lire les documents reçus au sujet de l'utilisation des technologies pédagogiques.

Stratégies de communication et de mobilisation

Pour assurer le succès de la campagne, il est primordial de transmettre l'information et les ressources au personnel, aux éducatrices et éducateurs ainsi qu'aux élèves (et à leurs parents). On encourage les conseils scolaires à faire participer leur service ou leur agente ou agent des communications et à l'informer des thématiques hebdomadaires.

Déterminez ensemble quels canaux utiliser lors de la campagne. Voici quelques exemples :

- Site Web ou Intranet du conseil scolaire;
- Comptes de médias sociaux du conseil;
- Affiches et documents papier (peut-être pas la meilleure option avec la pandémie);
- Courriels adressés au personnel, au corps enseignant et aux élèves;
- Discussions en classe;
- Autres outils dont dispose le conseil.

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

Sources utilisées

Les ressources de la campagne reprennent de l'information de nombreuses sources fiables en français et en anglais, disponibles en ligne :

- Centre d'excellence de l'Ontario pour la cybersécurité – https://www.ontario.ca/fr/page/centre-dexcellence-en-cybersecurite.
- Pensez cybersécurité (gouvernement du Canada) – https://www.pensezcybersecurite.gc.ca/fr.
- 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&lang=fr.
- GRC – 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/.
- White Ribbon – https://www.whiteribbon.ca/francais.html.
- Centre de toxicomanie et de santé mentale – https://www.camh.ca/fr/.
- Association pour la santé et l'éducation physique de l'Ontario – https://www.ophea.net/fr.
- UNICEF – https://www.unicef.org/fr.

Autres campagnes

En plus des thématiques et sujets abordés pendant la campagne MCS M-12, les conseils scolaires peuvent aussi employer les campagnes et ressources d'autres sources fiables. Certains thèmes et sujets pourraient être plus pertinents pour le personnel et ne pas traiter des trois piliers : la cybersécurité, la prudence et la confidentialité en ligne.

Voici deux campagnes dont les conseils scolaires devraient être mis au courant.

Division de la cybersécurité de l'Ontario

Mois de la sensibilisation à la cybersécurité – 2021 (lancement le 1er octobre)

Cette année marque le 10e Mois de la sensibilisation à la cybersécurité, qui a pour thème ***L'anatomie d'un piratage***. Chaque semaine en octobre, du nouveau contenu s'articulant autour d'un scénario de cyberattaque sera mis en ligne : bande dessinée romanesque en quatre parties, vidéos éducatives et questionnaires. Il enseignera aux participantes et participants comment se protéger d'une cybermenace. Le tout sera accessible gratuitement sur le site de l'événement.

Si cela vous intéresse, visitez le site de la campagne pour en savoir plus : https://cybersecurityontario.ca/mod/page/view.php?id=204&lang=fr_ca.

Les participantes et participants peuvent aussi s'inscrire pour recevoir les liens menant au nouveau contenu hebdomadaire et au contenu à venir. Cliquez sur le lien suivant pour vous inscrire : https://cybersecurityontario.ca/mod/page/view.php?id=171.

À noter que les activités de cette campagne sont peu personnalisables, et que le contenu sera publié une semaine à la fois en octobre.

Pensez cybersécurité (gouvernement du Canada)

Pensez cybersécurité est une initiative du gouvernement du Canada en place depuis de nombreuses années et dans le cadre de laquelle des campagnes et des ressources sur la cybersécurité sont préparées à l'intention de la population canadienne. Nombre de ces ressources ont d'ailleurs servi à monter la campagne MCS M-12.

Dans le cadre de cette initiative est organisé chaque année le Mois de la sensibilisation à la cybersécurité, lequel vise à informer le public de l'importance de la cybersécurité. Cette année, ce mois a pour thème « La vie en ligne ». Pour en savoir plus, consultez le site de l'initiative : https://www.pensezcybersecurite.gc.ca/fr/mois-de-la-sensibilisation-la-cybersecurite.

Pour connaître les thématiques hebdomadaires de la campagne, c'est par ici : https://www.pensezcybersecurite.gc.ca/fr/msc-thematiques.