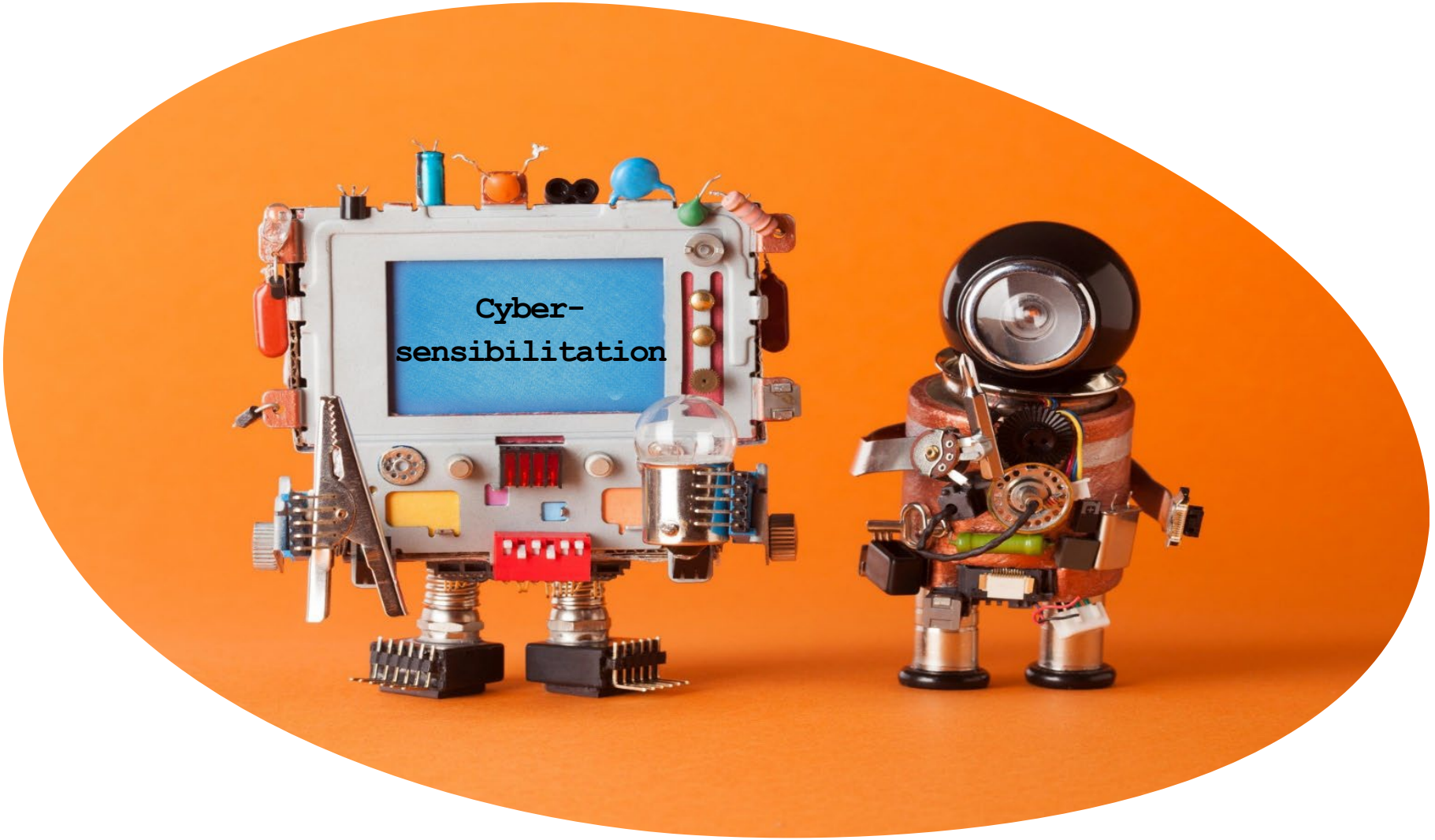


Calendrier de la cyber-sensibilisation M-12

Soyez cyberavertis!

Année scolaire 2021-2022

Ontario

2021

Septembre	Octobre	Novembre	Décembre
Cyber-sensibilisation pour la rentrée scolaire	Mois de la cyber-sensibilisation M-12	Nétiquette : Bonnes manières en ligne	Ne soyez pas victime d'une escroquerie en ligne!
			

2022

Janvier	Février	Mars	Avril
Pensez avant de cliquer...	Étranger DANGER!	Nettoyage printanier de l'espace numérique	Votre autodéfense numérique
			

Mai	Juin	Juillet	Août
Verrouillez votre porte, verrouillez vos données	Médias Sociaux	Jouez! En toute sécurité!	Objets connectés
			

Septembre 2021

Cyber-sensibilisation pour la rentrée scolaire

La rentrée scolaire est un moment excitant pour les étudiants, les parents, les enseignants et le personnel scolaire. Malheureusement, c'est aussi un moment convoité par les pirates informatiques, les voleurs d'identité et d'autres individus malhonnêtes, qui désirent profiter de cette période d'achalandage accrue. Parents : Il est important **d'être à l'affût des escroqueries de la rentrée scolaire**, et le mois de septembre est un mois parfait pour **rappeler aux enfants des moyens efficaces pour rester en sécurité en ligne** lors du retour à l'école.

Semaine 1: sept. 1 – 4

- **Conseils de la semaine 1 :** Effectuez une vérification de la sécurité en ligne et apprenez sur les moyens pour aider les enfants à être plus sécuritaires. Sécurisez les appareils, les comptes et les connexions de vos enfants. Si vous achetez un nouvel appareil, sécurisez-le!

Semaine 2: sept. 5 – 11

- **Conseils de la semaine 2 :** Apprenez des moyens de parler aux enfants pour qu'ils soient cyberavertis. Voici une liste de vérification de cybersécurité bien pratique et bien simple!

Semaine 3: sept. 12 – 18

- **Conseils de la semaine 3 :** Protégez les comptes et les mots de passe des plateformes d'apprentissage et des outils éducatifs fournis par l'école. En cas d'apprentissage à distance, n'oubliez pas les conseils de sécurité en matière de vidéoconférence pour les participants ou les éducateurs.

Semaine 4: sept. 19 - 25

- **Conseils de la semaine 4 :** Familiarisez-vous avez les politiques de la commission scolaire sur l'utilisation acceptable et le comportement en ligne. Soyez à l'affût des cybermessages importants de la part de la commission scolaire ou de l'école.

Semaine 5: sept. 26 – 30

- **Conseils de la semaine 5 :** Rappelez aux enfants les risques d'hameçonnage, le partage excessif de renseignements et l'utilisation excessive de la technologie. Testez leurs connaissances en matière de sécurité. Apprenez ce qu'il faut faire face à un message suspect.

Octobre 2021

Mois de la cyber-sensibilisation M-12

Le mois d'octobre est internationalement reconnu comme le mois de la cyber-sensibilisation. Notre campagne est adaptée à l'enseignement M-12 (maternelle à douzième année) et met l'accent sur la cybersécurité, la sécurité en ligne et la confidentialité en ligne. Le thème de cette année est « **Se renseigner sur la sécurité en ligne, c'est prendre soin de soi!** », avec des thèmes hebdomadaires supplémentaires. Adopter des habitudes sécuritaires et sécurisées en ligne, c'est prendre soin de sa présence en ligne et de son empreinte en ligne.

Semaine 1: oct. 3 – 9

- **Thème de la semaine 1 :** Prenez soin de vos appareils et de vos comptes.

Semaine 2: oct. 10 – 16

- **Thème de la semaine 2 :** Faites attention à votre réseau domestique et aux connexions Wi-Fi.

Semaine 3: oct. 17 – 24

- **Thème de la semaine 3 :** Prenez soin de vos renseignements personnels, car ils sont précieux!

Semaine 4: oct. 24 – 30

- **Thème de la semaine 4 :** Soyez conscient de votre présence en ligne et de votre empreinte numérique.

Novembre 2021

Nétiquette : bonnes manières en ligne

Nétiquette est la combinaison des mots **« net » (Internet)** et « **étiquette** », qui correspond à l'ensemble de règles pour la conduite acceptable en ligne. Nous avons besoin de ces règles pour savoir comment communiquer en ligne de manière respectueuse et comment utiliser l'Internet de manière productive, positive et socialement responsable. La **règle d'or de la nétiquette** est de traiter les gens en ligne comme vous souhaiteriez être traité.

Semaine 1: nov. 1 – 6

- **Conseils de la semaine 1 :** Partagez consciemment et avec respect. Si vous ne le diriez pas en personne, ne le dites pas en ligne. Évitez de publier des messages irrespectueux, incendiaires ou offensants en ligne.

Semaine 2: nov. 7 - 13

- **Conseils de la semaine 2 :** Ne publiez pas et ne partagez pas (même en privé) de contenu inapproprié. Tout ce que vous publiez ou partagez en ligne reste en ligne... pour toujours... **même si vous pensez l'avoir supprimé.** Connaissez la loi – Le partage non consensuelle d'une image intime n'est jamais acceptable! Si quelqu'un a partagé une photo de toi sans ton consentement, il y a des mesures que tu peux prendre.

Semaine 3: nov. 14 - 20

- **Conseils de la semaine 3 :** L'intimidation et le harcèlement peuvent se produire en ligne et peuvent être particulièrement dangereux, car ils sont plus faciles à pratiquer, plus visibles et suivent la victime. Apprenez-en davantage sur la cyberintimidation lors de la semaine de la sensibilisation à l'intimidation et de la prévention.

Semaine 4: nov. 21 - 27

- **Conseils de la semaine 4 :** Faites attention à votre ton. Utiliser DES MAJUSCULES, des points d'exclamation et l'humour peut être interprété à tort comme une forme d'impolitesse ou une grossièreté. Et oui, la grammaire et l'orthographe sont importantes.

Semaine 5: nov. 28 - 31

- **Conseils de la semaine 5 :** Publiez des choses inspirantes et qui motiveront les autres de manière positive. Ne soyez pas un pourvoyeur de désinformation et de fausses nouvelles. Vérifiez les faits avant de partager ou de repartager.

Décembre 2021

Ne soyez pas victime d'une escroquerie en ligne!

La fraude liée aux achats en ligne est le type le plus courant d'infraction contre les biens. Examinez vos achats avant de payer et recherchez les signaux d'alarme : est-ce que le prix est trop bas? Pas d'option de paiement par PayPal? Pas de conditions de remboursement ou de commentaires?

Semaine 1: déc. 1 – 4

- **Conseils de la semaine 1 :** Méfiez-vous des biens ou des services annoncés en ligne. Si l'affaire semble trop belle pour être vraie, c'est probablement le cas. Comment éviter d'être victime d'une fraude en magasinant en ligne.

Semaine 2: déc. 5 – 11

- **Conseils de la semaine 2 :** Les renseignements personnels figurant sur les médias sociaux sont faciles à obtenir pour les escrocs en ligne, qui peuvent les utiliser et effectuer des achats sans votre permission : connaissez et contrôlez ce que votre profil mentionne et affiche.

Semaine 3: déc. 12 – 18

- **Conseils de la semaine 3 :** Achetez-vous un logiciel en ligne? Vérifiez toujours ce que vous tentez de télécharger pour vous assurer que vous n'êtes pas dirigé vers un site ou un logiciel malveillant. Apprenez des moyens pour télécharger sécuritairement.

Semaine 4: déc. 19 – 25

- **Conseils de la semaine 4 :** Vous connectez-vous à un site Web légitime ou répondez-vous à un courriel légitime? Soyez attentifs aux signes de mystification, et ne vous faites pas avoir! Utilisez des sites Web sécurisés qui contiennent HTTP**S** au lieu de HTTP.

Semaine 5: déc. 26 – 31

- **Conseils de la semaine 5 :** Les cybercriminels recherchent constamment des moyens de frauder des individus sans méfiance. Voici quelques techniques favorites de cybercriminels et apprenez comment neutraliser la fraude.

Janvier 2022

Pensez avant de cliquer

Les cybercriminels utilisent souvent des adresses électroniques qui semblent correctes, des sujets d'actualité, des promesses de prix ou des gratuités pour nous inciter à cliquer sur des liens malveillants (mauvais). Ces criminels espèrent prendre les gens au dépourvu. Soyez prudent et réfléchissez aux messages que vous recevez avant de cliquer.

Semaine 1: janv. 2 – 8

- **Conseils de la semaine 1 :** Ne vous laissez pas convaincre de partager vos renseignements confidentiels, comme vos mots de passe, ou de télécharger des logiciels malveillants.

Semaine 2: janv. 9 – 15

- **Conseils de la semaine 2 :** Apprenez sur l'hameçonnage, et ne mordez pas à l'hameçon. Avant de fournir toute information, essayez de vérifier par un autre canal de communication que l'expéditeur est bien celui qu'il prétend être.

Semaine 3: janv. 16 – 22

- **Conseils de la semaine 3 :** Envisagez d'installer un logiciel antivirus et anti-maliciel qui analyse les fichiers à la recherche de certaines tendances ou signatures de virus et de logiciels malveillants connus. Protégez-vous!

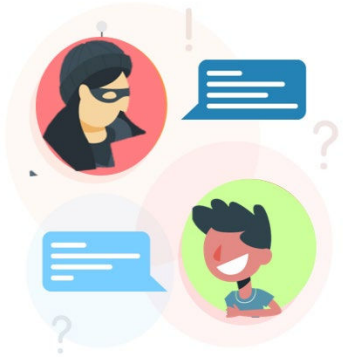
Semaine 4: janv. 23 – 29

- **Conseils de la semaine 4 :** Méfiez-vous des rançongiciels qui peuvent prendre le contrôle de votre appareil et verrouiller vos accès ou vos fichiers. Apprenez comment assurez votre cybersécurité.

Février 2022

Étranger, DANGER!

Méfiez-vous des personnages inconnus en ligne, procédez avec prudence et faites extrêmement attention aux renseignements personnels que vous révélez. Les prédateurs en ligne peuvent mentir à propos de tout. Avant de vous engager avec de nouveaux « amis » en ligne, demandez-vous : cette personne est-elle vraiment qu'un simple étranger?



Semaine 1: févr. 1 – 5

- **Conseils de la semaine 1 :** Faites attention aux prédateurs en ligne. Ils renforcent votre confiance en vous envoyant beaucoup de messages, vous demandent de garder vos conversations secrètes et vous manipulent pour obtenir vos renseignements personnels.

Semaine 2: févr. 6 – 12

- **Conseils de la semaine 2 :** N'oubliez pas de vérifier les demandes d'amis et les invitations de groupe avant de les accepter. Demandez-vous si vous avez fait passer un « nouvel ami » au statut de « non-étranger » trop rapidement.

Semaine 3: févr. 13 – 19

- **Conseils de la semaine 3 :** Utilisez les contrôles de sécurité pour personnaliser la cyberexpérience de votre famille, bloquer les contenus inappropriés et établir des limites de temps. Établissez des règles de base, et parlez des risques et des moyens de les atténuer.

Semaine 4: févr. 20 – 26

- **Conseils de la semaine 4 :** Soyez conscient des risques de leurre par Internet et de conditionnement, et faites attention aux cappers. Un enfant victime peut montrer des changements de comportement à la maison et à l'école, reconnaissez les signes. Apprenez-en davantage sur la traite des personnes.

Mars 2022

Nettoyage printanier de l'espace numérique

Le printemps est arrivé! C'est l'heure d'un nettoyage numérique. Saviez-vous que les espaces numériques ont besoin d'être nettoyés, tout comme nos maisons? L'encombrement numérique peut ralentir les appareils et les services que vous utilisez. La conservation d'anciens fichiers, comptes en ligne et programmes /applications peut mettre vos appareils et vos renseignements en danger. Pour assurer la sécurité de vos appareils et de vos données tout au long de l'année, prenez le temps de faire un nettoyage printanier de votre espace numérique.

Semaine 1: mars 1 – 5

- **Conseils de la semaine 1 :** Supprimez les applications/programmes inutilisés et obsolètes sur vos appareils. Cela permet de libérer de l'espace et d'éviter que de vieux renseignements soient partagés. Certaines applications obsolètes peuvent également devenir non sécuritaires.

Semaine 2: mars 6 – 12

- **Conseils de la semaine 2 :** Passez vos comptes en revue et fermez/supprimez ceux que vous n'utilisez pas. Cela réduit le risque d'exposer vos renseignements personnels (courriels, noms d'utilisateur, mots de passe, etc.) en cas de violation de données.

Semaine 3: mars 13 – 19

- **Semaine 3 Tips:** Clear your web browser cache and cookies. This improves web browser performance and increases your online privacy.

Semaine 4: mars 20 – 26

- **Conseils de la semaine 3 :** Effacez la mémoire cache et les témoins de votre navigateur Web. Cela permet d'améliorer les performances du navigateur Web et de renforcer votre confidentialité en ligne.

Semaine 5: mars 27 – 31

- **Conseils de la semaine 5 :** Mettez à jour vos systèmes et logiciels. Le fait de disposer des dernières mises à jour permet de sécuriser vos appareils et vos renseignements. Recyclez-vous votre appareil? Sachez ce qu'il faut faire.

Avril 2022

Votre autodéfense numérique

Des détails tels que les dates de naissance, les numéros de téléphone, les comptes bancaires, l'éducation, la sexualité, les affiliations religieuses, les adresses électroniques et les mots de passe sont régulièrement révélés en ligne, laissant les internautes vulnérables à l'ingénierie sociale et éventuellement à la cybercriminalité. L'autodéfense numérique est une question d'autonomisation numérique. Apprenez des stratégies numériques pour protéger vos renseignements personnels, votre image et votre réputation en ligne.

Semaine 1: avr. 3 – 9

- **Conseils de la semaine 1 :** Vérifiez les paramètres de confidentialité/sécurité de vos appareils et protégez les renseignements personnels sur les applications mobiles, car elles peuvent envoyer des données et utiliser votre microphone pour « écouter » des renseignements.

Semaine 2: avr. 10 – 16

- **Conseils de la semaine 2 :** Les renseignements personnels que vous publiez en ligne peuvent vous exposer, vous et vos proches, à un risque accru de cybercriminalité et de harcèlement. Les planifications de voyage et les photos peuvent indiquer aux voleurs que vous êtes absent!

Semaine 3: avr. 17 – 23

- **Conseils de la semaine 3 :** Il est possible que vous partagiez sans le savoir des renseignements personnels par le biais de jeux et de questionnaires sur les médias sociaux, ainsi que des photos et des messages interactifs et partageables. Combattez l'envie et la pression des pairs!

Semaine 4: avr. 24 – 30

- **Conseils de la semaine 4 :** Protégez votre réputation. Les données créées par vos activités et vos communications en ligne constituent votre empreinte numérique. Cela comprend les « j'aime » et les commentaires.

Mai 2022

Verrouillez votre porte, verrouillez vos données

Si vous ne quittez pas votre maison sans verrouiller votre porte, il devrait en être de même pour vos appareils, vos applications et vos comptes. Les mots de passe ou les phrases passe constituent la première ligne de défense contre les intrus et les cybercriminels. Quelques bonnes pratiques en matière de mots de passe vous aideront à protéger vos appareils, vos comptes et vos renseignements personnels. Prenez le temps de le faire, cela en vaut le coup!

Semaine 1: mai 1 - 7

- **Conseils de la semaine 1 :** Utilisez toujours un mot de passe ou phrase passe sécuritaire et unique pour chaque compte et chaque appareil. N'utilisez pas de renseignements personnels (p. ex., nom, âge, date de naissance, nom de votre enfant, nom de votre animal de compagnie).

Semaine 2: mai 8 - 14

- **Conseils de la semaine 2 :** Vérifiez la force de tous vos mots de passe. Vérifiez si vos mots de passe ont déjà été sujets à une violation de données. Si oui, modifiez-les!

Semaine 3: mai 13 - 21

- **Conseils de la semaine 3 :** Utilisez un gestionnaire de mots de passe pour conserver la trace des renseignements de connexion. Ne permettez jamais à votre navigateur d'enregistrer vos mots de passe. Désactivez le gestionnaire de mots de passe intégré à votre navigateur.

Semaine 4: mai 22 - 28

- **Conseils de la semaine 4 :** Vérifiez si l'authentification multifactorielle (MFA) est disponible sur vos appareils et vos comptes. Si oui, établissez-la pour améliorer la sécurité. N'oubliez pas de ne pas partager vos données de connexion et votre mot de passe.

Juin 2022

Médias sociaux

L'utilisation des médias sociaux vous permet d'entrer en contact avec vos amis et votre famille, de partager vos intérêts avec d'autres personnes ou de vous informer sur les dernières nouvelles. **Bien que les médias sociaux peuvent être amusants, ils peuvent également être risqués!** Partager vos renseignements personnels peut faire de vous une cible facile pour les fraudeurs, les voleurs d'identité et les prédateurs en ligne. C'est pourquoi vous devez toujours être vigilant à propos de ce que vous partagez en ligne!

Semaine 1: juin 1 – 4

- **Conseils de la semaine 1 :** Vos amis en ligne sont-ils ceux qu'ils prétendent être? Soyez sélectif, soyez prudent, et soyez perspicace! Faites toujours attention aux personnes avec lesquelles vous vous connectez. Bloquez les connexions non amicales.

Semaine 2: juin 5 – 11

- **Conseils de la semaine 2 :** Quels sont vos paramètres de confidentialité sur vos appareils et vos applications de médias sociaux installées? Privatisez votre vie sociale en définissant des autorisations de confidentialité.

Semaine 3: juin 12 – 18

- **Conseils de la semaine 3 :** Ne partagez pas tout sur les médias sociaux, surtout vos renseignements personnels.

Semaine 4: juin 19 – 25

- **Conseils de la semaine 4 :** N'utilisez pas les services de localisation, surtout lorsque vous publiez en ligne. Évitez de fournir trop de renseignements sur vos activités, cela pourrait permettre d'exposer votre position exacte.

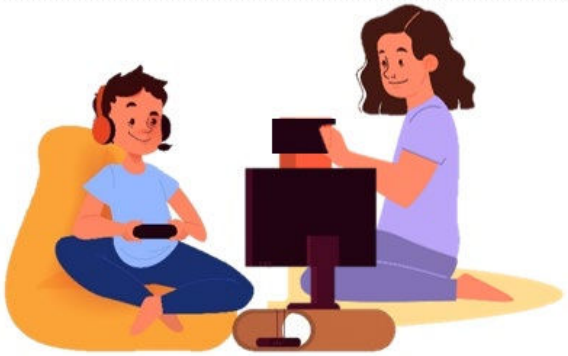
Semaine 5: juin 26 – 30

- **Conseils de la semaine 5 :** Soyez judicieux quant à ce que vous publiez en ligne. Vous représentez ce que vous publiez, et les publications sont éternelles! Soyez prévenant et demandez l'autorisation avant de publier des renseignements sur les autres.

Juillet 2022

Jouez! En toute sécurité!

Les jeux en ligne sont amusants pour les enfants comme pour les adultes! Ils peuvent être encore plus amusants lorsque vous jouez avec sagesse, en toute sécurité et que vous savez quand vous arrêter. Aujourd'hui, la plupart des jeux sont en ligne ou connectés à l'Internet. Cela rend les joueurs vulnérables aux attaques de cybercriminels ou au harcèlement provenant d'individus malveillants. Découvrez comment faire en sorte que votre expérience de jeu en ligne soit sécuritaire et agréable.



Semaine 1: juill. 3 – 9

- **Conseils de la semaine 1 :** Passez en revue les comptes de jeu pour configurer les paramètres de confidentialité et de sécurité afin de limiter le partage excessif de renseignements. Définissez un contrôle parental pour établir des paramètres pour les enfants.

Semaine 2: juill. 10 – 16

- **Conseils de la semaine 2 :** Jouez déguisé, utilisez un avatar et un nom d'utilisateur de jeu sécuritaire. N'utilisez pas votre photo, votre prénom, votre nom ou tout autre détail personnel.

Semaine 3: juill.17 – 23

- **Conseils de la semaine 3 :** Pensez aux personnes avec lesquelles vous jouez. Les gens ne sont pas forcément honnêtes à propos de leur identité. Bloquez, signalez et mettez en sourdine les personnes qui vous harcèlent dans les jeux.

Semaine 4: juill. 24 – 30

- **Conseils de la semaine 4 :** Faites attention aux achats dans les jeux et aux lots aléatoires (loot boxes). Ne téléchargez pas de logiciels provenant d'inconnus, comme des logiciels de triche ou des scripts et programmes d'automatisation, car ils peuvent contenir des logiciels malveillants.

Août 2022

Objets connectés

Les montres intelligentes, les haut-parleurs intelligents, les sonnettes intelligentes, les systèmes de sécurité domestique, les caméras intelligentes, les appareils électroménagers intelligents et même les toilettes intelligentes (clin d'œil) rendent notre vie plus pratique... Toutefois, ils peuvent être utilisés par des cybercriminels s'ils ne sont pas sécurisés. Découvrez comment sécuriser ces appareils contre les cybermenaces.

Semaine 1: août 1 – 6

- **Conseils de la semaine 1 :** Modifiez les noms d'utilisateur et les mots de passe par défaut! Conservez vos appareils intelligents sur un réseau distinct.

Semaine 2: août 7 – 13

- **Conseils de la semaine 2 :** Maintenez à jour les logiciels de vos appareils intelligents. Appliquez les mises à jour automatiquement ou veillez à les vérifier et à les effectuer régulièrement.

Semaine 3: août 14 – 20

- **Conseils de la semaine 3 :** Avant d'acheter un appareil intelligent, renseignez-vous sur les renseignements personnels qu'il collecte et sur les contrôles de confidentialité qu'il offre.

Semaine 4: août 21 – 27

- **Conseils de la semaine 4 :** Faites vos recherches avant d'acheter un jouet intelligent : recueille-t-il et partage-t-il des renseignements d'identification? Le jouet et les renseignements qu'il recueille peuvent-ils être efficacement sécurisés?

Semaine 5: août 28 – 31

- **Conseils de la semaine 5 :** Avez-vous un assistant numérique domestique? Réglez ses paramètres de confidentialité. Utilisez-vous un appareil portatif, tel qu'un moniteur d'activité physique ou une montre intelligente? Découvrez les risques pour la vie privée.

Résumé des cyberressources référencées

Septembre 2021 – Cyberprotection pour la rentrée scolaire

- Semaine 1 :
  - Répondez aux questions de l'examen Pensez cybersécurité – *Pensez cybersécurité, Gouvernement du Canada*
  - Le guide des parents pour le magasinage de la rentrée en toute cybersécurité – *Pensez cybersécurité, Gouvernement du Canada*
  - Sécurisez vos appareils – *Pensez cybersécurité, Gouvernement du Canada*
  - Sécurisez vos comptes – *Pensez cybersécurité, Gouvernement du Canada*
  - Sécurisez vos connexions – *Pensez cybersécurité, Gouvernement du Canada*
  - Liste de conseils pour un nouvel appareil – *Pensez cybersécurité, Gouvernement du Canada*
- Semaine 2 :
  - Comment les parents doivent-ils aborder ce sujet avec leurs enfants ? – *Pensez cybersécurité, Gouvernement du Canada*
  - Liste de vérification de cybersécurité – *Pensez cybersécurité, Gouvernement du Canada*
- Semaine 3 :
  - Des conseils pour une vidéoconférence sécurisée pour le personnel et les enseignants
  - Des conseils pour une vidéoconférence sécurisée pour les participants
- Semaine 5 :
  - Vidéo : Hameçonnage: ne mordez pas! – *Pensez cybersécurité, Gouvernement du Canada*
  - De vrais exemples de faux courriels – *Pensez cybersécurité, Gouvernement du Canada*
  - Devine quoi!?! – CyberJulie (zoeandmolly.ca) – *Centre canadien de protection de l'enfance*
  - Que faire d'un message qui vous semble suspect – *Pensez cybersécurité, Gouvernement du Canada*

Octobre 2021 – Mois de la cyber-sensibilisation M-12

- Mois de la cyber-sensibilisation (MCS) M-12 2021 – *ecno.org*
- Semaine 1 : MCS M-12 2021 – Semaine 1 - *ecno.org*
- Semaine 2 : MCS M-12 2021 – Semaine 2 - *ecno.org*
- Semaine 3 : MCS M-12 2021 – Semaine 3 - *ecno.org*
- Semaine 4 : MCS M-12 2021 – Semaine 4 - *ecno.org*

Novembre 2021 – Nétiquette : Bonnes manières en ligne

- Semaine 3 :

    - Semaine de la sensibilisation à l'intimidation et de la prévention – *Gouvernement de l'Ontario*
    - Cyberintimidation : Comment rester en sécurité – *Kids Help Phone*
- Semaine 5 : Faux que ça cesse - *HabiloMédias*

Décembre 2021 – Ne soyez pas victime d'une escroquerie en ligne!

- Semaine 1 : Comment éviter d'être victime d'une arnaque en magasinant en ligne – *Pensez cybersécurité, Gouvernement du Canada*
- Semaine 2 : Réseaux sociaux - Pensez cybersécurité (pensezcybersecurite.gc.ca) – *Pensez cybersécurité, Gouvernement du Canada*
- Semaine 3 : Comment assurer notre cybersécurité lorsqu'on télécharge ou utilise une application – *Pensez cybersécurité, Gouvernement du Canada*
- Semaine 4 : Introduction à la mystification – *Pensez cybersécurité, Gouvernement du Canada*
- Semaine 5 :
    - Un bref survol des tactiques préférées des cybercriminels – *Pensez cybersécurité, Gouvernement du Canada*
    - À bas l'arnaque – Protégez-vous contre la fraude - Canada.ca – *Gouvernement du Canada*

Janvier 2022 – Pensez avant de cliquer...

- Semaine 1 : Comment se fait-on leurrer par les cybermenaces? Le piratage psychologique. – *Pensez cybersécurité, Gouvernement du Canada*
- Semaine 2 : Qu'est-ce que l'hameçonnage? – *Pensez cybersécurité, Gouvernement du Canada*
- Semaine 3 :
    - Maliciel détecté! – *Pensez cybersécurité, Gouvernement du Canada*
    - Qu'est-ce qu'un maliciel et comment vous en protéger? – *Pensez cybersécurité, Gouvernement du Canada*
- Semaine 4 :
    - Vidéo: Maliciels et rançongiciels – *Pensez cybersécurité, Gouvernement du Canada*
    - Rançongiciel 101 : Comment assurer votre cybersécurité – *Pensez cybersécurité, Gouvernement du Canada*

Février 2022 – Étranger, DANGER!

- Semaine 4 :
    - Leurre par internet – *cyberaide.ca*
    - Le conditionnement – *cyberaide.ca*
    - La dure vérité : Les cappers : qui sont-ils et quel danger représentent-ils pour les jeunes internautes? – *Parentscyberavertis.ca*

- Signes qu'une personne peut être victime de la traite des personnes – *Gouvernement de l'Ontario*
- Traite des personnes – *Gouvernement de l'Ontario*

Mars 2022 – Nettoyage printanier de l'espace numérique

- #SCRUB...vos appareils méritent un grand ménage – *Pensez cybersécurité, Gouvernement du Canada*
- Semaine 2 : Just Delete Me | Un annuaire de liens pour supprimer vos comptes de sites webs - *backgroundchecks.org*
- Semaine 3 : Astuces pour votre navigateur Web – *ecno.org*
- Semaine 4 :
  - Avez-vous un plan de sauvegarde pour vos données? – *Pensez cybersécurité, Gouvernement du Canada*
- Semaine 5 :
  - Mises à jour de systèmes – *Pensez cybersécurité, Gouvernement du Canada*
  - Vidéo : Mises-à-jour aux logiciels – *Pensez cybersécurité, Gouvernement du Canada*
  - Recycler votre appareil – *Recyclemycell.ca*

Avril 2022 – Votre autodéfense numérique

- Semaine 1 :
  - Protection des renseignements personnels stockés dans vos appareils mobiles - *Commissariat à la protection de la vie privée du Canada*
  - Conseils pour protéger vos renseignements personnels lors du téléchargement et de l'utilisation d'applications mobiles - *Commissariat à la protection de la vie privée du Canada*

Mai 2022 – Verrouillez votre porte, verrouillez vos données

- Semaine 1 : Phrases de passe, mots de passe et NIP – *Pensez cybersécurité, Gouvernement du Canada*
- Semaine 2 :
  - How Secure Is My Password? (Quel est le niveau de sécurité de mon mot de passe) (site en anglais seulement)
  - Have I Been Pwned? (Est ce que mon mot de passe est compromis?) (site en anglais seulement)
- Semaine 3 : Gestionnaires de mots de passe – *Pensez cybersécurité, Gouvernement du Canada*
- Semaine 4 : Pourquoi l'authentification multifactorielle constitue-t-elle un élément essentiel de la cybersécurité? – *Pensez cybersécurité, Gouvernement du Canada*

Juin 2022 – Média sociaux

- Semaine 1 : Vos amis en ligne sont-ils bien ceux qu'ils prétendent? - *Commissariat à la protection de la vie privée du Canada*

- Semaine 2 : Conseils pour utiliser les paramètres de confidentialité – Média sociaux et autres services en ligne - *Commissariat à la protection de la vie privée du Canada*

Juillet 2022 – Jouez! En toute sécurité!

- Consoles de jeu – *Pensez cybersécurité, Gouvernement du Canada*

Août 2022 – Objets connectés

- Comment sécuriser vos appareils intelligents contre les cybermenaces cet été – *Pensez cybersécurité, Gouvernement du Canada*
- Semaine 1 : Les appareils intelligents et la protection de la vie privée – Protégez le réseau - *Commissariat à la protection de la vie privée du Canada*
- Semaine 2 : Les appareils intelligents et la protection de la vie privée – La sécurité : bien plus que l'affaire de quelques secondes - *Commissariat à la protection de la vie privée du Canada*
- Semaine 5 :
    - Conseils pour utiliser les paramètres de confidentialité – Assistants numériques domestiques - *Commissariat à la protection de la vie privée du Canada*
    - Les accessoires intelligents et votre vie privée - *Commissariat à la protection de la vie privée du Canada*

Résumé des cyberévénements annuels

- Octobre 2021 – Cyber Security Awareness Month (CSAM) and K-12 Cyber Awareness Month (CAM)
- 25 au 30 octobre 2021 – Semaine éducation médias
- 22 au 26 novembre 2021 – Semaine de la sensibilisation à l'intimidation et de la prévention
- 28 janvier 2022 – Journée de la protection des données
- 8 février 2022 – Journée pour un Internet plus sûr
- 22 février 2022 – Journée de sensibilisation à la traite de personne
- Mars 2022 – Mois de la prévention de la fraude
- 20 mars 2022 – Digital Cleanup Day (La journée du nettoyage numérique) (site en anglais seulement)
- 31 mars 2022 – La journée mondiale de la sauvegarde

- 17 juin 2022 – Journée pour l'élimination de la cyberintimidation en Ontario

Ce calendrier a été mise au point avec collaboration de représentants du Ministère de l'Éducation, du Réseau informatique éducationnel de l'Ontario (RIEO), de conseils scolaires membres du comité consultatif des technologies de l'intormation et des communications (CCTIC) et d'OASBO ICT (Ontario Association of School Business Officials Information and Communication Technology), et avec la contribution de la Division de la cybersécurité de l'Ontario du Ministère des services gouvernementaux et Services aux consommateurs, et Pensez cybersécurité du Gouvernement du Canada.