Encourager la sensibilisation à la cybersécurité tout au long de l'année!

Ontario

Thèmes mensuels sur la cyber-sensibilisation

Septembre

Cyberhygiène

Sensibilisation à la cybersécurité pour une rentrée scolaire sécuritaire et bien organisée!

Octobre

Mois de la cyber-sensibilisation

Encourager des pratiques plus sûres et plus sécuritaires dans les communautés scolaires sur l'utilisation de technologie et d'Internet en faisant la promotion des pratiques exemplaires entourant la cybersécurité et la protection de la vie privée en ligne, de la maternelle à la 12e année.

Novembre

La bienveillance en ligne

Explorer les ramifications de la cyberintimidation et souligner l'importance d'être un internaute respectueux et aimable.

Décembre

Arnaques et hameçonnage

Tout sur les activités malveillantes en ligne utilisées pour duper les gens afin de les dérober et d'obtenir leurs renseignements personnels.

Janvier

Préservez la confidentialité de vos renseignements!

L'importance de gérer et de protéger vos renseignements personnels en ligne.

Février

Pédopiégeage en ligne

L'importance de demeurer vigilant et de se protéger contre les prédateurs en ligne qui essayent d'attirer des enfants et des jeunes à des fins d'exploitation sexuelle.

Mars

Sauvegarde de données

Gérer son empreinte numérique en maintenant un mode de vie numérique sain en désencombrant son espace numérique et en sauvegardant ses données.

Avril

Jouer en sécurité dans le métavers

Maintenir le côté divertissant des jeux en ligne en étant conscient des dangers et des menaces.

Mai

Bien-être numérique

Encourager l'adoption de saines habitudes dans l'utilisation de la technologie et en connaissant ses limites pour maintenir un mode de vie sain.

Juin

Médias sociaux

L'importance d'être proactif pour se protéger des dangers potentiels que posent les médias sociaux.

Juillet

Nettoyage numérique

L'importance de supprimer les applications et les comptes que nous n'utilisons plus pour maintenir un environnement numérique sans risque.

Août

Maisons connectées

La technologie de maison intelligente procure des bienfaits au quotidien, et il est important de savoir comment bien utiliser ces genres de technologies.

Ontario

Septembre

Cyberhygiène

Sensibilisation à la cybersécurité pour la rentrée scolaire

Cyberhygiène: pour assurer la sûreté des appareils

Les ordinateurs, téléphones et tablettes stockent tous des renseignements personnels convoités par les cybercriminels. Il est important de sécuriser adéquatement ses appareils en respectant les règles de base de la cyberhygiène pour éviter que ses informations tombent en de mauvaises mains.

Voici quelques conseils :

- Installer un **antivirus** et un **anti-logiciel espion**, la première ligne de défense con¬tre les cybercriminels.
- Activer la mise à jour automatique – les mises à jour peuvent être programmées pour être téléchargées et l'installées la nuit.
- Consulter régulièrement les **paramètres de confidentialité** et limiter les informations que les autres peuvent voir.
- Verrouiller les appareils à l'aide de **l'empreinte digitale**, la reconnaissance faciale, d'un **code** ou d'un **mot de passe**.
- Garder les **paramètres de navigateurs** à jour et effacer régulièrement les **données de navigation**.

Soyez cybervigilante et cybervigilant

Pour beaucoup, la rentrée scolaire est un moment excitant. Malheureusement, les cybercriminels en profitent d'exploiter les jeunes peu familiers avec les risques en ligne. Pensez à aborder les sujets suivants avec les enfants:

1. Les cybercriminels, qui sont-ils et que veulent-ils?
2. Que font-ils avec nos informations?
3. Comment se protéger?

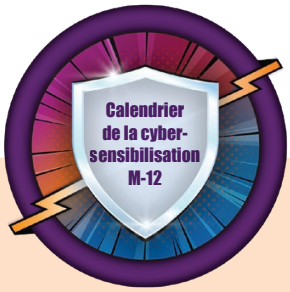
Se protéger en utilisant des mots de passe ro¬bustes et l'authentification multifactorielle

La rentrée scolaire est une bonne occasion de se rap¬peler ce qui fait la sûreté **d'un bon mot de passe.** Voici quelques conseils:

1. Choisir un **mot de passe long**, préférablement de 15 caractères ou plus.
2. Combiner **MAJUSCULES, minuscules, $ymbo!es et n0mbr3s pour renforcer un mot de passe**.
3. Utiliser une phrase secrète pour créer un mot de passe significatif et facile à retenir. Une phrase secrète est une suite de mots comme «MonAdor¬ableHamsterGustave» ou «BasketballÉquipeDeFeu».

En plus du mot de passe, on peut utiliser l'authentifica¬tion multifactorielle (AMF) pour améliorer la sécurité de ses comptes. L'AMF repose sur une combinaison de fac¬teurs pour authentifier une utilisatrice ou un utilisateur.
Exemples de facteurs :

- **Une chose qu'on sait** – comme un mot de passe ou une phrase secrète.
- **Une chose qu'on a** – tel qu'un téléphone ou un jeton.
- **Une chose propre à soi** – tel qu'une empreinte digitale.



Pour plus d'informations : www.ecno.org/cyber-sensibilisation

Ontario

Novembre

La bienveillance en ligne

Les trois indispensables de la cybersécurité:

1. Traiter les autres comme on voudrait être traité.
2. Réfléchir avant de publier ou d'envoyer un message.
3. Dénoncer immédiatement l'intimidation.

Cyberintimidation

La cyberintimidation, c'est blesser ou humilier intentionnellement quelqu'un en ligne. Les conséquences peuvent être graves et de longues durées, car il n'y a pas d'espace sûr. La cyberintimidation peut survenir n'importe quand et n'im¬porte où, et rapidement vu par un grand nombre de personnes.

Exemples de cyberintimidation:

- Envoyer des courriels ou des messages haineux ou menaçants.
- Diffuser des photos de quelqu'un de nature gênante ou sexuelle.
- Se faire passer pour quelqu'un d'autre en utilisant son nom.
- Raconter des potins, des secrets, des rumeurs ou des mensonges.

Effets sur la victime:

- Sentiment de solitude, tristesse, peur, frustration, colère.
- Perceptions négatives de soi, de ses amis et de sa vie.
- Volonté d'éviter l'école, les activités et tout autre endroit où elle peut être reconnue

Que peut-on faire?

Opter pour la prudence:

- **Protéger sa vie privée:** Régler les paramètres de confidentialité sur les médias sociaux et ne pas divulguer ses informations ou ses mots de passe.
- **Savoir qui sont ses amis:** Choisir attentivement qui on accepte et restreindre ce que les amis d'amis ou le public peuvent voir ou accéder.
- **Demander de l'aide:** En cas d'erreur, d'inquiétude ou de cyberintimidation, en parler à un parent ou à un adulte de confiance.

Faire preuve de bienveillance

- Ne pas envoyer ou publier de messages blessants.
- Traiter les gens avec respect.
- Complimenter les autres de manière constructive et appropriée.

Si tu es victime de cyberintimidation

- Ne réplique pas par des méchancetés.
- Bloque la personne et cesse toute communication avec elle.
- Préviens un parent, un adulte de confiance, l'école, le site ou l'appli, ou la police.

Si tu es témoin de cyberintimidation

- N'aime pas et ne partage pas les messages – cela pourrait empir-er la situation.
- Si tu connais l'intimidatrice ou l'intimidateur et te sens à l'aise de le faire, dis-lui qu'il n'y a pas de place pour la cyberintimidation.
- Demande de l'aide à un adulte de confiance.

Calendrier de la cyber-sensibilisation M-12

Pour plus d'informations : www.ecno.org/cyber-sensibilisation

Ontario

Décembre

Arnaques et hameçonnage

Ne soit pas victime de fraude!

Une cyberarnaque est une activité criminelle en ligne conçue pour soutirer des gens de l'argent ou des informations personnelles.

Les types de fraudes les plus communs

L'hameçonnage (aussi connu comme du «phishing» ou «smishing») est une technique visant à récolter (ou «pêcher») des noms d'utilisatrice ou d'utilisateur, des mots de passe et d'autres renseignements confidentiels auprès de plusieurs (ou dans une «mer») d'utilisa-trices et utilisateurs – par courriel ou texto. Ces courriels et textos frauduleux semblent provenir d'une personne ou d'une entreprise connue ou fiable.

- Ces messages incitent la destinatrice ou le destinataire à cliquer sur un lien, ouvrir un fichier, composer un numéro ou correspondre à une adresse courriel.
- On piège ensuite la victime afin qu'elle fournisse ses renseignements personnels et données d'authentification.

Les fausses applications sont des applications créées par des cybercriminels pour causer du tort aux utilisatrices et utilisateurs et à leurs appareils. Elles sont conçues pour ressembler à de vraies applications, mais contrairement, elles suivent tes activités, installent un logiciel malveillant ou soutirent tes informations.

Les sites web qui vendent de faux produits. Ces sites offrent des produits en forte demande à rabais que la personne qui achète ne recevra jamais.

Le détournement de formulaire est le piratage d'un site web commercial légitime qui redirige les clientes et clients vers une fausse page de paiement. De cette page le fraudeur peut soutirer les renseignements personnels et les numéros de carte de crédit.

Comment éviter la fraude en ligne:

- Ne pas ouvrir les pièces jointes, cliquer sur les liens ou répondre à un message suspect – pose-toi des questions, consulte des personnes en qui tu as confiance ou communique avec l'expéditrice ou l'expéditeur en utilisant une autre méthode de communication.
- Éviter les applications suspectes et ne pas accorder la permission à une application de faire quelque chose qu'elle n'est pas censée faire.
- Toujours utiliser des sites sécurisés **(doit contenir le «s» dans https://)** lorsque tu magasines ou que tu dois te connecter à un compte en ligne.
- Acheter des produits de commerces connus seulement.
- Ne pas publier d'informations personnelles sur les médias sociaux.

Si tu penses être victime d'une arnaque:

- Cesse toute communication avec la personne frauduleuse.
- Demande de l'aide à une ou un adulte de confiance.
- Signale la fraude à la police.

Calendrier de la cyber-sensibilisation M-12

Pour plus d'informations : www.ecno.org/cyber-sensibilisation

Ontario

Janvier

Préservez la confidentialité de vos renseignements!

Gestion des paramètres de confidentialité et de sécurité sur vos appareils mobiles

Voici des astuces:

- **Limitez la quantité de renseignements personnels stockés dans vos appareils.**
- Utilisez des **mots de passe robustes** et des **fonctions de verrouillage automatique** pour empêcher les accès non autorisés à vos appareils mobiles.
- Évitez d'utiliser **les points d'accès sans fil publics** pour les transactions qui utilisent des renseignements personnels ou financiers. Utilisez plutôt un VPN ou vos données cellulaires.
- Téléchargez des applications uniquement sur **les sites autorisés**.
- **Vérifiez les autorisations** d'une application lors de son installation pour savoir à quels renseignements l'application peut accéder dans votre appareil.
- Vérifiez fréquemment vos **paramètres de localisation** pour savoir quelles applications vous surveillent.

« Partager ou ne pas partager : telle est la question. »

C'est toujours agréable de planifier un voyage et de faire toute sorte d'activités pendant ses vacances. Cela dit, il est judicieux d'attendre d'être rentré chez vous avant de publier des photos et des vidéos. En annonçant votre départ sur les réseaux sociaux, vous indiquez aux voleurs que vous ne serez pas à la maison.

Gare à l'excès d'information

Il est important de savoir quels types de renseignements peuvent être **partagés en ligne**. C'est normal de partager votre nom, votre emplacement et votre âge avec vos amies et amis, mais vous ne devriez jamais partager publiquement votre adresse, votre date de naissance complète ou votre géolocalisation.

Protection de votre réputation

Tout ce que vous publiez en ligne ou par message texte fait maintenant partie de votre identité. Voici quelques conseils qui vous aideront à protéger votre réputation en ligne :

- **L'internet n'oublie jamais.** Lorsque vous clavardez ou que vous publiez en ligne, rappelez-vous que rien n'est temporaire.
- Vérifiez fréquemment vos **paramètres de confidentialité** et assurez-vous que votre profil est **privé**. De cette façon, vos publications ne seront pas visibles aux personnes en dehors de votre profil.
- Ne publiez jamais de photos inappropriées ou **intimes**.
- Ne répondez jamais aux **demandes inappropriées.**
- Si une situation vous dérange, **déconnectez-vous** et réfléchissez à la façon dont vous voulez aborder la situation et discutez-en avec un adulte de confiance.

Calendrier de la cyber-sensibilisation M-12

Pour plus d'informations : www.ecno.org/cyber-sensibilisation

Ontario

Février

Pédopiégeage en ligne

Le pédopiégeage en ligne consiste à utiliser des moyens technologiques (des réseaux sociaux, des sites de jeu, des salles de clavardage, etc.) pour inciter des personnes mineures à participer à des activités à caractère sexuel contre leur gré.

- **Une prédatrice ou un prédateur** peut se faire passer pour une amie ou un ami de l'école, l'ami(e) d'un ami(e) ou quelqu'un que vous avez rencontré lors d'une activité parascolaire.
- Elle ou il peut faire usage de **flatterie** ou de **compliments** pour se rapprocher de vous, ou encore avoir recours à **l'intimidation**, au **harcèlement** ou **aux menaces** pour contrôler vos interactions.
- Elle ou il pourrait vous **promettre des cadeaux** comme un nouveau téléphone, une tablette électronique, de l'argent, des drogues ou de l'alcool.
- Elle ou il peut compatir avec les difficultés dont vous avez fait part en ligne. Par exemple, des problèmes à la maisonafin de gagner votre confiance.
- Elle ou il peut vous envoyer des **photos inappropriées** pour vous inciter à envoyer des photos ou des vidéos semblables en retour. Cela peut **mener à du chantage**, où elle ou il menacera de les envoyer à vos ami(e)s ou à votre famille.

Que faire si quelqu'un essaie de vous attirer

- Parlez-en à un adulte de confiance.
- Si vous avez besoin d'aide immédiatement, appelez le **911**.
- Pour signaler un cas d'exploitation sexuelle et obtenir de l'aide, appelez la **Ligne d'urgence canadienne contre la traite des personnes au 1-833-900-1010** ou Tchat **www.canadianhumantraffickinghotline.ca**

Conseils de sécurité en ligne

- Vérifiez les **demandes d'amis** et les **invitations de groupe** avant de les accepter. Regardez si vous avez des ami(e)s en commun et ne vous sentez pas obligé de les accepter.
- Ne partagez pas de **renseignements personnels** lors de vos interactions en ligne.
- Évitez les **publications** qui indiquent des **problèmes** à la maison ou à l'école; cela peut permettre à une prédatrice ou un prédateur de profiter de votre situation ou de vos sentiments.
- Si on vous offre quelque chose qui semble **trop beau pour être vrai** (comme de **l'argent** ou un **nouveau téléphone**), c'est proba¬blement le cas. Parlez-en à un adulte de confiance.
- Ne **partagez jamais votre adresse** et évitez de rencontrer des personnes que vous avez connues en ligne sans en parler avec un adulte de confiance.

Calendrier de la cyber-sensibilisation M-12

Pour plus d'informations : www.ecno.org/cyber-sensibilisation

Ontario

Mars

Sauvegarde de données

Désencombrez et sauvegardez vos données

Notre vie numérique est animée de nombreuses activités, de la navigation au clavardage en passant par la publication de photos et de vidéos. Ces divers comptes, applications et appareils laissent une empreinte numérique qui facilite le travail des cybercriminels et met en danger nos renseignements personnels.

En plus de posséder de multiples comptes et applications, nous générons aussi énormément de données. Cela peut ralentir nos appareils électroniques et accroître les risques de perdre des fichiers importants.

Afin d'assurer la sécurité de nos données et de nos appareils, il est important de maintenir une bonne hygiène numérique, notamment en désencombrant notre environnement numérique et en sauvegardant nos données.

Liste de nettoyage de vos appareils

Faites un nettoyage de vos appareils électroniques comme les téléphones et les portables avec les conseils suivants:

- Supprimez les applications que vous n'utilisez pas fréquemment.
- Supprimez votre historique de navigation et d'appels.
- Examinez vos photos et vos vidéos et supprimez celles qui sont floues, inutiles ou en double.
- Archivez vos vieux courriels.
- Désabonnez-vous des infolettres que vous ne lisez pas.

Liste des données à sauvegarder

Évitez les pertes de données inutiles avec les conseils suivants:

- Examinez et triez régulièrement vos photos, vidéos, documents, courriels et autres fichiers importants.
- Enregistrez et sauvegardez fréquemment vos fichiers.
- Considérez effectuer une sauvegarde de vos données sur un autre emplacement comme un disque externe ou en stockage infonuagique.

L'importance du nettoyage et de la sauvegarde

- **Paix d'esprit:** Inutile de craindre une défaillance de vos appareils si vos fichiers sont sauvegardés ailleurs.
- **Espace suffisant:** En supprimant les fichiers et les applications inutiles, vous ne manquerez pas d'espace sur vos appareils.
- **Données sécurisées:** En ayant moins d'applications et de comptes, vos données sont moins accessibles sans votre autorisation.
- **Appareils de haute performanc**e: En nettoyant les données sur votre appareil, vous améliorerez la performances et la durée de vie de la batterie de l'appareil.
- **Moins de pollution numérique:** Les fichiers et les données inutiles sont des déchets numériques. Ceux-ci contribuent à la pollution numérique qui augmente la consommation d'énergie. En les supprimant, vous économisez de l'électricité.

Pour plus d'informations : www.ecno.org/cyber-sensibilisation

Ontario

Avril

Jouer en sécurité dans le métavers

Jouer en ligne en toute sécurité

C'est tellement amusant de jouer en ligne avec ses ami(e)s! Malheureusement, les cybercriminels se servent aussi des jeux pour voler les renseignements personnels des joueuses et joueurs. Voici quelques conseils pour jouer en ligne de façon sécuritaire:

- N'inclus pas ton nom, ton **âge**, une **photo de toi** ou n'importe quel autre **élément permettant de t'identifier** dans ton avatar.
- Garde tes appareils et tes applications, particulièrement tes logiciels antivirus et antimaliciels, à jour en installant les dernières mises à jour.
- Choisis des jeux **classés pour ton groupe d'âge** (les classifications sont là pour te protéger).
- Utilise un **mot de passe** (ou une phrase de passe) pour protéger tes comptes.
- N'utilise que des sites fiables pour télécharger des jeux.

Le métavers, c'est quoi?

Le métavers est un monde virtuel - semblable au monde réel dans lequel les gens peuvent interagir sous la forme de personnages virtuels en 3D à l'aide d'un casque de réalité virtuelle (RV). On peut télécharger des applications pour y jouer, clavarder ou simplement être entre amis. C'est intéressant et amusant, mais ce n'est pas un lieu sans risques.

Les risques du métavers et les moyens de se protéger

- **Les gens peuvent dissimuler leur identité réelle.** N'importe qui peut se cacher derrière un avatar. Des adultes peuvent se faire passer pour des adolescentes ou adolescents afin de t'attirer vers un espace privé et t'envoyer du contenu graphique inapproprié. **Sois prudente ou prudent lorsque tu rencontres des gens en ligne.**
- Le métavers n'est pas un lieu modéré. C'est aux utilisatrices et utilisateurs de signaler le contenu inapproprié ou dérangeant, y compris les cas de **cyberintimidation**, de **racisme** et de **harcèlement sexuel.** Il est important de savoir comment signaler ces situations ou de parler à un parent ou à un **adulte de confiance** pour savoir quoi faire si tu te retrouves dans une **situation inappropriée ou dérangeante.**

Conseils pour les parents

- Le métavers **n'est pas conçu pour les enfants** de moins de 13 ans et ne filtre pas le contenu selon l'âge.
- Les applications et les appareils de RV et de réalité augmentée (RA) ont quelques **contrôles parentaux** et **paramètres** de **confidentialité**; prenez le temps de les découvrir.
- L'accès au métavers se fait par un appareil de RV/RA. Comme il n'y a **aucune visibilité** de l'extérieur, c'est-à-dire qu'on ne peut pas voir ce qui s'y passe pour intervenir, il est essentiel d'avoir un **dialogue ouvert** sur ce qui se passe dans le métavers.

Calendrier de la cyber-sensibilisation M-12

Pour plus d'informations : www.ecno.org/cyber-sensibilisation

Ontario

Mai

Bien-être numérique

Pour une utilisation saine de la technologie

Le bien-être numérique, vise à faire la promotion des habitudes saines qui nous permettent de conserver une bonne hygiène de vie lors de l'utilisation des technologies.

Améliorer notre bien-être numérique

- **Rester actif:** Les enfants et les jeunes de 5 à 17 ans devraient faire 60 minutes d'activité physique modérée à intense par jour.
- Limiter **le temps passé devant les écrans** à des fins récréatives (pas en lien avec l'école) à 2 heures par jour.
- **Dormir suffisamment:** Les enfants de 5 à 13 ans ont besoin de 9 à 11 heures de sommeil par jour pour être bien reposés; ceux de 14 à 17 ans ont besoin de 8 à 10 heures par jour pour une bonne hygiène de vie.
- **Développer des relations saines:** Les enfants doivent apprendre à socialiser avec les autres et comprendre des perspectives et des identités dif¬férentes afin de développer l'écoute, le respect et l'empathie.
- **Parler de ses émotions quant aux activités en ligne:** Il faut encourager les enfants à parler avec un parent ou un adulte de confiance de leurs activités en ligne et à se confier s'ils vivent des situations problématiques.

La nature comme remède

On dit que la nature a des effets positifs sur la santé, menant à des améliorations au sens global sur la santé mentale, l'estime de soi, la gestion du stress et la résilience. Des recherches ont démontré que passer deux heures ou plus par semaine en nature augmentait les chance d'être en bonne santé et d'améliorer son bien-être. Voici quelques façons de renouer avec la nature:

- **Déconnectez-vous** de la technologie et prenez une pause d'écran.
- Allez faire une **promenade** dans un parc ou en forêt.
- Étendez-vous dans l'herbe et regardez les nuages au **son de la nature.**

Obtenir de l'aide

Obtenir du soutien confidentiel et gratuit en ligne grâce à Jeunesse, J'écoute à **https://jeunessejecoute.ca/**

Obtenir du soutien confidentiel et gratuit au téléphone grâce à Jeunees, J'écoute à **1 800 668- 6868** ou par texto au **686868**

Calendrier de la cyber-sensibilisation M-12

Pour plus d'informations : www.ecno.org/cyber-sensibilisation

Ontario

Juin

Médias sociaux

À l'aube des vacances d'été, protégez-vous et protégez vos renseignements en ligne

L'été est arrivée et les médias sociaux sont parfaits pour garder contact avec les amies, amis et la famille. Il est important de rester proactif et de se protéger des dangers des médias sociaux. Pour utiliser ces derniers de manière sécuritaireé, voici quelques conseils simples à suivre.

Comment utiliser les médias sociaux de façon sécuritaire

1. Assurez-vous que vos publications sont privées et ne peuvent être vues que par vos contacts.
2. Vérifiez souvent vos paramètres de confidentialité, surtout après la mise à jour d'une application.
3. Réfléchissez avant de publier en ligne. Garder l'information suivante confidentielle:
   - **Renseignements personnels** – Ne partagez pas votre numéro de téléphone, votre adresse ou votre date de naissance complète .
   - **Emplacement** – Assurez-vous de ne pas partager votre emplacement et supprimez les étiquettes de géolocalisation de vos vieilles photos .
   - **Activités de la vie** – Ne publiez pas vos photos de vacances ou d'événements avant d'être de retour à la maison.
   - **Renseignements financiers** – Ne publiez jamais de renseignements bancaires en ligne ou ceux liés à des achats.
   - **Nouvelles sur la vie des autres** – Faites attention à ce que vous partagez à propos de vos amies, amis et de votre famille. Demandez toujours leur autorisation.

Se défaire de l'anxiété de ratage et de déconnexion

L'anxiété de ratage (aussi appelé syndrome FOMO) est caractérisée par la peur de ne pas savoir ce que font vos amies, amis et l'impression de rater l'occasion de s'amus¬er avec eux.

L'anxiété de déconnexion (aussi appelé syndrome FOBO) est la peur d'être décon¬necté du monde virtuel.

Pour surmonter ces sentiments:

- Concentre-toi sur les relations positives et significatives, les **interactions en per¬sonne et les expériences réelles** à l'extérieur des médias sociaux (par exemple, faire une randonnée, une promenade en vélo ou une sortie au cinéma).
- **Ta valeur** n'est pas liée au nombre de mention « J'aime » que tu reçois en ligne. Les autres ne sont pas plus intéres¬sants que toi simplement parce qu'ils reçoivent plus de mention « J'aime » en ligne.
- Souviens-toi **les photos et les vidéos** ne sont qu'une partie de la vie des autres, et elles sont souvent très modifiées.
- Suis des personnes qui **t'inspirent**, qui **encouragent le positivisme** et le **bonheur** et qui ont des choses à t'appren¬dre! Apprends à filtrer le contenu qui nuit à ton bien-être.
- Si tu ne te sens pas bien, parles-en à un parent, à une amie ou un ami ou à un adulte de confiance.

Calendrier de la cyber-sensibilisation M-12

Pour plus d'informations : www.ecno.org/cyber-sensibilisation

Ontario

Juillet

Ménage d'été

Rafraîchir son espace numérique

Applis et programmes inutilisés

Faites l'inventaire des applications sur votre téléphone ou votre ordinateur. Les avez-vous toutes utilisées récemment? Supprimez celles qui ne servent plus pour libérer de l'espace et empêcher que de vieux renseignements soient partagées. Pour ne pas courir de risques, mieux vaut se débarrasser des applications obsolètes qui pourraient être non sécurisées.

Un compte, deux comptes, trois comptes...

Il est important de fermer ou de supprimer les comptes qui ne servent plus pour mieux protéger votre confidentialité et vos données.

Voici quelques façons de trouver vos comptes:

- Faites une **recherche** de votre nom et de vos adresses courriel.
- Consultez votre **gestionnaire de mots de passe** pour voir les comptes inutilisés.
- Fouillez vos **vieux courriels.**
- Regardez si votre **navigateur** contient de vieux noms d'utilisateur ou mots de passe.
- Vérifiez les **médias sociaux** pour trouver d'anciens comptes.

Effacer le cache et les fichiers témoins

Les sites Web stockent beaucoup de données en mémoire locale et dans le navigateur, ce qui représente une cible attrayante pour les pirates informatiques. Il est important d'effacer le cache et les fichiers témoins pour améliorer votre confidentialité.

Pour vous protéger, vous pouvez:

- Personnalisez les paramètres de sécurité de votre **navigateur** pour qu'il supprime les **fichiers témoins** lorsque vous le fermez.
- Évitez d'enregistrer vos **identifiants** dans un navigateur.
- Désactivez la fonction de **remplissage automatique** pour vos renseignements personnels.

Déchets électroniques

Que sont les déchets électroniques? Tous les appareils électroniques qui ne servent plus sont des déchets électroniques. Heureusement, on peut les donner ou les recycler pour éviter qu'ils se retrouvent au dépotoir.

Types de déchets électroniques qui peuvent être donnés ou recyclés:

- Ordinateurs.
- Téléphones intelligents et tablettes.
- Appareils photo numériques et lecteurs multimédias.
- Accessoires (imprimantes, écrans, disques externes, clés USB .
- Consoles de jeu.

Avant de donner ou de recycler vos appareils:

- Sauvegardez vos données sur un autre appareil ou dans le nuage.
- Supprimez les données de manière permanente.
- Retirez les disques durs et les cartes mémoire.

Faites une recherche en ligne pour savoir où jeter vos déchets électroniques dans votre région.

Pour plus d'informations : www.ecno.org/cyber-sensibilisation

Ontario

Août

Maisons connectées

Chez soi en toute sécurité

Des objets, des objets et encore des objets

Les maisons intelligentes sont de plus en plus courantes de nos jours, avec divers appareils de l'Internet des objets (IdO) – téléviseurs, thermostats, ampoules, appareils ménagers et même les prises électriques accessibles à partir d'un téléphone intelligent. Ces formidables appareils, permettent aux gens de rester connectés et en contrôle de leur maison. Mais avoir un accès facile à divers appareils facilite également l'accès aux renseignements personnels pour les pirates informatiques. Pour demeurer connecté en toute sécurité, voici quelques éléments à garder en tête.

Vulnérabilités des maisons intelligentes

- **Réseaux sans fil et routeurs non sécurisés** – Les pirates peuvent passer par des réseaux sans fil et des routeurs non sécurisés pour pirater les maisons intelligentes.
- **Appareils à sécurité minimale** – De nombreux **appareils IdO** ne sont pas conçus pour être mis à jour, ce qui les rend vulnérables aux cyberattaques.
- Les caractéristiques de **sécurité** ne sont pas toujours **activées** par défaut.

Meilleures stratégies pour sécuriser vos appareils IdO et votre maison intelligente

- **Connectez les appareils IdO à un câble Ethernet,** si possible, plutôt qu'à un réseau sans fil. Autrement, assurez-vous que ce réseau est protégé par un mot de passe.
- Modifiez le et nom le **mot de passe par défaut** de votre réseau sans fil et de votre routeur. Les mots de passe par défaut sont faibles et faciles à pirater.
- **Limitez-vous aux appareils IdO essentiels** dans votre maison plutôt qu'aux appareils que vous voulez) – considérez les risques de piratage de chaque appareils. Quel niveau de risque êtes-vous prêt à assumer?
- Allez vers des **marques et produits de confiance.** Consultez les renseignements et les commentaires sur les produits en ligne. Assurez-vous que les appareils intègrent des caractéristiques de sécurité.
- **Utilisez l'authentification à deux facteurs,** si disponible – cette mesure renforce la sécurité. En plus d'un nom d'utilisateur et d'un mot de passe, une deuxième méthode de vérification s'ajoute, comme un code envoyé par téléphone.
- Gardez vos **appareils et applications à jour.** Installez les dernières mises à jour sur vos appareils et applications.

Calendrier de la cyber-sensibilisation M-12

Pour plus d'informations : www.ecno.org/cyber-sensibilisation

Ontario

Comprendre l'IA :
systèmes génératifs, risques et meilleures pratiques

Qu'est-ce que l'intelligence artificielle (IA)?

Il s'agit d'une technologie qui permet aux ordinateurs d'effectuer des tâches qui requièrent habituellement l'intellect humain, comme comprendre une langue, reconnaître des modèles et prendre des décisions. Elle peut contribuer à l'automatisation des tâches, à l'amélioration de la créativité, à la résolution de problèmes complexes et à la recherche, au divertissement, à l'éducation et à bien d'autres domaines.

L'IA est déjà présente dans de nombreux aspects de notre vie quotidienne. Exemples :

- **applications photo** pour améliorer la qualité des images et reconnaître des personnes;
- **recommandations d'achat en ligne** basées sur l'historique de navigation et d'achat;
- des **robots conversationnels automatisés de service à la clientèle** qui aident à répondre aux questions;
- **recommandations de contenu sur les médias sociaux** basées sur vos activités en ligne;
- **reconnaissance des visages** sur les médias sociaux pour mentionner des amis;
- les **systèmes domotiques** tels que les thermostats intelligents et les systèmes de sécurité;
- les **applications de navigation** qui analysent le trafic et suggèrent des itinéraires optimaux;
- les systèmes de **détection des fraudes** utilisés par les banques pour détecter les activités de dépenses inhabituelles;
- les **réponses suggérées** dans les applications de courriel et de messagerie.

Qu'est-ce que l'IA générative?

Il s'agit d'une sous-catégorie de l'IA qui permet de créer du contenu, tel que du texte, du code, des images, de la musique, de l'audio, de la vidéo et de l'animation. Les capacités de l'IA générative continuent de s'étendre grâce aux progrès technologiques.

Rappel : L'IA est un outil puissant qui peut être aussi fascinant qu'utile. Cependant, celle-ci comporte des risques, et il convient de l'utiliser de manière judicieuse et responsable!

Risques potentiels de l'IA générative :

- **La mésinformation :** L'IA peut créer ou propager des renseignements incorrects.
- **La dépendance :** Une dépendance excessive à l'égard de l'IA peut nuire à la pensée critique et la créativité.
- **Préoccupations en matière de confidentialité :** Certains outils d'IA peuvent collecter des renseignements personnels.
- **Préjugés :** si elle n'est pas correctement formée, l'IA peut promouvoir ou renforcer des préjugés.
- **Manque de transparence :** La manière dont l'IA crée son contenu et les sources qu'elle utilise ne sont pas entièrement comprises.
- **Risques liés aux droits d'auteur :** La question de savoir qui détient les droits d'auteur sur le contenu créé par l'IA fait l'objet d'un débat continu.
- **Autres risques potentiels :** L'IA évolue rapidement, et il est possible que certains risques ne soient pas entièrement connus ou compris.
- **Considérations éthiques et culturelles :** L'IA suscite des préoccupations éthiques, si elle crée du contenu fondé sur des connaissances culturelles ou autochtones, celui-ci est-il considéré comme de l'appropriation culturelle?

Exemples de meilleures pratiques pour utiliser l'IA :

- **Comprendre l'outil d'IA et le modèle de données** qu'il utilise, ainsi que son fonctionnement, ses points forts et ses limites.
- **Utilisation éthique et responsable :** Respecter les lois en matière de droits d'auteur. Veiller à ce que l'IA ne soit pas utilisée pour produire ou diffuser du contenu protégé par des droits d'auteur sans autorisation. Ne pas utiliser l'IA à des fins de tromperie ou de mésinformation.
- **Vérifier les renseignements :** Vérifier toujours l'exactitude, la pertinence et la qualité du contenu créé par l'IA.
- **Rester curieux :** Utiliser l'IA comme un outil pour faciliter et compléter l'apprentissage, la créativité et le jugement, et non pour les remplacer. Ne pas utiliser l'IA de manière excessive.
- **La confidentialité d'abord :** Il convient de faire preuve de prudence lors du partage de renseignements personnels ou de données sensibles avec des plateformes d'IA. Toujours lire et comprendre la politique de confidentialité du service ou de la plateforme d'IA.
- **Comprendre les limites :** L'IA est un outil, et non une solution parfaite. Il faut toujours réfléchir de manière critique à ses résultats et remettre en question les informations créées. Sont-elles exactes? Sont-elles appropriées? Sont-elles éthiques?
- **Créditer de manière appropriée :** Faire mention de l'utilisation de l'IA dans les projets.

Pour plus d'informations : www.ecno.org/cyber-sensibilisation

Ontario