LA LIBERTÉ
Depuis 1913

Clinique de Cyber-Criminologie

GÉNÉRATION CYBER-SMART

INFORMATIONS PERSONNELLES ****

Sous ce thème, nous visons à enseigner aux enfants ce qui constitue des informations personnelles, ce qui peut et ne peut pas être partagé sur Internet, comment les informations sont partagées en ligne et quels sont les risques associés. Nous pensons qu'il est important que les enfants sachent que même si le partage d'informations peut être un moyen de s'intégrer dans la culture en ligne et d'obtenir plusieurs avantages en retour, comme la possibilité de rester en contact avec ses amis en ligne, d'avoir accès à des jeux et à des plateformes sociales, et plus encore, assurer la sécurité de leurs informations demeure leur responsabilité.

generationcybersmart.ca

Un projet rendu possible financièrement grâce à :

Secrétariat aux relations canadiennes Québec

Société de la francophonie manitobaine

QU'EST-CE QU'UNE INFORMATION PERSONNELLE?

Les informations personnelles dénotent un concept très large qui, en termes simples, se définit par tout ce qui se rapporte à soi-même, de son prénom à l'historique de son navigateur Web. Hors ligne, il n'est pas toujours évident de savoir comment ces informations peuvent être utilisées contre nous ou au profit d'autres personnes, mais en ligne, où les données peuvent être plus facilement collectées et agrégées, c'est une autre histoire. Voici quelques exemples de catégories d'informations personnelles :

- **Identifiants de base** : Il s'agit de détails tels que le nom complet, la date de naissance, le sexe et le numéro d'assurance sociale.
- **Coordonnées personnelles** : Les informations telles que l'adresse à la maison, l'adresse courriel, le numéro de téléphone et d'autres coordonnées sont considérées comme des informations personnelles.
- **Informations financières** : Les détails concernant votre situation financière, tels que les numéros de comptes bancaires et les informations relatives aux cartes de crédit et aux revenus entrent dans cette catégorie. Certaines de ces informations peuvent être obtenues à partir de vos habitudes en ligne, comme vos choix d'achats en ligne et les groupes dont vous êtes membre sur les réseaux sociaux, par exemple.
- **Informations sur la santé** : Ceci inclut les données relatives à la santé ou aux antécédents médicaux d'une personne, y compris les dossiers médicaux, les prescriptions et les informations relatives à l'assurance maladie. En ligne, vous avez peut-être partagé certaines de ces informations en achetant des lunettes de vue, en discutant avec un médecin sur une plateforme de télémédecine, en recherchant des symptômes, en adhérant à un club de santé ou en achetant des produits liés à la santé, par exemple.
- **Données biométriques** : Les données biométriques, telles que les empreintes digitales, les données de reconnaissance faciale et les scans rétiniens, sont également considérées comme des informations personnelles. Si vous avez utilisé Ancestry ou 23AndMe, leurs bases de données contiennent des informations sur votre ADN, qui peuvent être incluses dans cette catégorie.
- **Identifiants en ligne** : Les noms d'utilisateur, mots de passe, adresses IP et autres identifiants en ligne font partie des informations personnelles.
- **Informations de localisation** : En termes simples, il s'agit de toute information permettant de savoir où vous vous trouvez, que ce soit grâce aux données de localisation directement collectées par votre téléphone ou aux informations collectées par les tours cellulaires lorsque vous passez un appel téléphonique.

- **Informations sur le mode de vie** : Ce type d'informations comprend les lieux que vous fréquentez le plus, comme votre lieu de travail et votre épicerie locale, les produits que vous achetez le plus souvent, le type de voiture que vous conduisez, votre historique de navigation, etc.
- **Informations sociales et démographiques** : Les détails concernant le milieu social, l'origine ethnique, l'état civil et d'autres informations démographiques d'une personne sont inclus dans cette catégorie.
- **Informations sur la voix et l'image** : À l'ère de l'intelligence artificielle, votre voix et votre image peuvent également être considérées comme des informations personnelles.

COMMENT LES INFORMATIONS SONT-ELLES PARTAGÉES?

Les informations personnelles **peuvent être partagées en ligne** de plusieurs manières, souvent dans le cadre d'activités en ligne courantes. Il suffit parfois de remplir un formulaire ou un sondage, ou de se créer un compte : dans ces exemples, les informations sont ouvertement demandées à l'utilisateur, indiquant clairement les informations qu'il donne - son nom, son adresse électronique, sa date de naissance, etc. Il en va de même pour vos transactions en ligne, lorsque vous êtes invité à saisir vos informations financières et votre adresse postale.

Vous pouvez aussi partager vos informations sans être directement invité à le faire. Par exemple, lorsque vous publiez un message sur les réseaux sociaux à propos d'une crèmerie que vous avez visitée avec votre famille, vous partagez un endroit où on peut vous trouver, vos préférences personnelles, avec qui vous vous trouvez, etc. Il en va de même pour les photos et les vidéos que vous téléversez dans une application de type album photo numérique, par exemple, ou les messages que vous envoyez par messagerie instantanée, par courriel ou sur des plateformes d'assistance à la clientèle : tous ces systèmes accumulent des informations que vous leur transmettez volontairement.

Si vous souhaitez approfondir cette notion avec vos élèves pour mieux illustrer la manière dont ils partagent des informations personnelles lors de leurs activités quotidiennes en ligne, vous pouvez leur montrer des photos de personnes au hasard (il peut s'agir d'une photo que vous avez vous-même publiée en ligne!) ou des captures d'écran de profils de réseaux sociaux. Demandez à vos élèves de dresser la liste de toutes les informations qu'ils peuvent découvrir sur la personne en se basant sur cette image ou ce profil. Porte-t-elle une casquette de l'école qu'elle a fréquentée? La photo a-t-elle été prise devant la bibliothèque locale, indiquant que cette personne habite peut-être dans le coin? Utilisez cet exercice pour leur démontrer tout ce qu'ils partagent eux-mêmes peut-être avec le monde.

POURQUOI FAIRE ATTENTION LORSQU'ON PARTAGE SES INFORMATIONS PERSONNELLES EN LIGNE? QUELS SONT LES RISQUES?

Tel que démontré, plusieurs informations peuvent être utilisées pour nous identifier alors qu'on préfèrerait les garder privées. Elles peuvent donc également être utilisées par des **individus malveillants**, et ce, contre notre volonté. La chose la plus importante à retenir est que, même si vous pensez que vos informations sont en sécurité en ligne, il n'y a aucune garantie qu'elles le soient. Dans le cadre du contrat social qui nous permet d'utiliser l'internet et la variété d'outils qui y sont disponibles, **nous acceptons de renoncer à une certaine vie privée, et donc à certaines informations personnelles**.

Le risque le plus inquiétant est celui d'être piraté parce que de nombreux systèmes comportent des **vulnérabilités**. Cela signifie que, tout comme votre compte Facebook peut être repris par un pirate si votre mot de passe est divulgué ou craqué, les systèmes d'une entreprise peuvent être piratés, rendant les informations qu'ils détiennent sur vous vulnérables à une **utilisation malveillante**.

Bien sûr, vos informations financières sont peut-être les plus critiques, car les fuites de données bancaires vous exposent directement à des **pertes financières ou des vols d'identité** qui peuvent ne pas être facilement résolus, mais il y a d'autres façons dont vos informations personnelles peuvent être utilisées contre vous. Par exemple, si votre adresse courriel ou votre numéro de téléphone sont divulgués publiquement en ligne, les fraudeurs sont plus susceptibles d'essayer de vous envoyer des courriels ou des appels d'hameçonnage, voire de vendre ou de regrouper ces informations avec d'autres pour en tirer profit.

Les enfants sont susceptibles de partager des informations en ligne, car ils n'ont pas encore appris à distinguer ce qui est trop personnel pour être partagé de ce qui ne l'est pas. Ils s'exposent ainsi à toutes sortes de risques, y compris le conditionnement ou *grooming* en ligne, le piratage ou même des menaces pour leur sécurité, s'ils communiquent par erreur leur adresse ou les lieux qu'ils fréquentent souvent.

Les études montrent que les jeunes enfants sont plus enclins à publier du contenu en ligne, comme de courtes vidéos ou des photos, ils peuvent donc également être la cible de fraudeurs utilisant des outils d'hypertrucage. L'hypertrucage est le terme donné à la manipulation de contenu (souvent vidéo ou audio) avec l'aide d'outils d'IA pour leur donner une apparence réaliste alors que ce contenu est en fait fictif. C'est une technique utilisée tant dans des cas de fraude falsifiant la voix d'un enfant pour obtenir de l'argent d'un membre de sa famille que dans des cas plus graves où de la pornographie juvénile a été créée à partir d'images de jeunes du secondaire.

En résumé, aucun système n'est à l'abri du piratage, plus nous éparpillons nos informations personnelles en ligne, plus elles sont recueillies, plus nous sommes susceptibles d'être la cible de personnes mal intentionnées en ligne.

QU'EST-CE QUI PEUT ET NE PEUT PAS ÊTRE PARTAGÉ EN LIGNE?

Nous ne souhaitons pas aviser qu'aucune information ne doit être partagée en ligne - après tout, non seulement est-ce un exploit impossible, mais cela rendrait l'internet très ennuyeux, voire complètement inutile. Cela est particulièrement vrai pour les enfants, qui ont beaucoup à gagner à pouvoir explorer et faire preuve de curiosité sur internet.

Dans nos ressources vidéo, nous expliquons aux enfants qu'ils peuvent partager certains détails d'identification de base, comme leur prénom, leur signe du zodiaque et leur lieu de résidence général, comme le nom de leur ville.

Cependant, en nous adressant à leurs adultes de confiance, il nous est important de nuancer ce conseil. Si votre élève porte un nom très particulier, ou si vous enseignez dans une petite ville, vous devrez peut-être lui dire de garder ces détails secrets en ligne, car ils pourraient être trop spécifiques et permettre à des inconnus en ligne de trouver facilement plus d'informations sur l'enfant.

C'est particulièrement vrai lorsqu'il s'agit d'un passe-temps ou d'un intérêt commun : un enfant vivant dans un petit village peut être facilement trouvé sur le site web de l'équipe de hockey locale, par exemple, le rendant vulnérable si quelqu'un de mal intentionné le cherche en ligne.

Dans ces cas-ci, nous recommandons particulièrement la **création d'un alter ego** pour l'enfant avec un nom ou un surnom différent et d'utiliser la grande ville la plus proche de la vôtre au lieu de dévoiler l'endroit où il demeure vraiment.

En revanche, les enfants ne devraient pas communiquer leur adresse complète, que ce soit dans un message envoyé sur un jeu en ligne ou en publiant une photo d'eux devant leur maison, ni leur numéro de téléphone à la maison.

En ce qui concerne les informations financières, de nombreux experts recommandent aux parents d'acheter des **cartes de crédit prépayées ou des cartes-cadeau** pour les transactions en ligne de leurs enfants plutôt que d'utiliser les informations de leur propre carte de crédit afin de limiter les conséquences en cas de fuite des détails de la carte.

En ce qui concerne les adresses courriel, la question de savoir s'il faut ou non les partager est moins tranchée. En théorie, nous ne devrions pas partager nos adresses courriel avec n'importe qui, car elles sont un moyen de communication directe avec soi. Mais en pratique, il est presque impossible de naviguer sur internet - ou même dans le monde réel - sans partager son adresse électronique.

C’est pourquoi nous recommandons de mettre en place un **système d’adresses multiples** : créez un compte de messagerie qui restera privé et qui ne sera utilisé que pour des comptes de haute importance, comme ceux utilisés pour les opérations bancaires et avec le gouvernement ; un compte qui sera utilisé pour les opérations secondaires, comme la connexion aux réseaux sociaux, les communications avec la famille, les amis et l’école ; et enfin, un compte utilisé comme une adresse de messagerie pour s’inscrire à des infolettres, à des concours, obtenir des codes promotionnels pour des sites d’achat en ligne, etc., mais qui ne contiendra pas beaucoup d’informations critiques puisqu’il sera le plus susceptible d’être compromis, vu la nature publique de son utilisation. En mettant vous-même en place ce système, et en le recommandant aux parents et aux élèves, vous prenez toutes les mesures à votre disposition pour avoir une base solide et sécuritaire en ce qui concerne les communications électroniques.

Comme mentionné précédemment, les jeunes enfants sont susceptibles de vouloir publier du contenu en ligne, ce qui les expose au risque que des fraudeurs falsifient leur image ou leur voix.

Bien qu’il soit important de parler à vos élèves du contenu qu’ils publient, pensez à ce que vous et votre école publiez sur les élèves et évitez vous aussi de publier trop de contenu à leur sujet. Parlez aux parents des risques que comportent la publication de contenu au sujet de leurs enfants, comme le risque de création de pornographie juvénile à l’aide d’outils d’intelligence artificielle, et assurez-vous qu’ils sont au courant de ces risques avant de publier.

COMMENT LIMITER LES INFORMATIONS DIFFUSÉES PUBLIQUEMENT?

Si vos élèves ont accès aux réseaux sociaux et que vous ne savez pas comment ajuster les paramètres de confidentialité pour limiter la visibilité de leurs informations, vous pouvez les diriger vers les paramètres de leurs comptes afin de les ajuster.

Le site Resolock a mis à la disposition du public gratuitement **six guides** pour sécuriser ses informations sur les plateformes de réseaux sociaux les plus populaires au Canada. Ces guides contiennent des captures d'écran et des explications étape par étape pour chacun des paramètres de sécurité que vous pourriez vouloir utiliser.

RESSOURCES

Resolock : https://www.resolock.com/

Centre de confidentialité Facebook : https://www.facebook.com/privacy/center/

Page sécurité Instagram : https://about.instagram.com/fr-fr/safety

Guide sur la sécurité et la confidentialité sur Snapchat :
https://www.internetmatters.org/fr/hub/guidance/snapchat-safety-a-how-to-guide-for-parents/

Menu sécurité et protection X (Twitter) :
https://help.twitter.com/fr/safety-and-security

Centre de sécurité et protection de la vie privée TikTok :
https://www.tiktok.com/safety/fr-fr/safety-privacy-controls/

Centre de sécurité Discord (anglais): https://discord.com/safety

Guide pour les parents sur Discord :
https://www.internetmatters.org/fr/hub/esafety-news/parents-guide-to-discord-on-how-your-kids-can-use-it-safely/#:~:text=La%20plateforme%20Discord%20est%2Delle,options%20de%20chat%20en%20ligne.

GLOSSAIRE

- **Informations personnelles** : Les informations personnelles sont des données qui identifient ou peuvent être utilisées pour identifier une personne, comme son nom et son adresse physique.
- **Données de localisation** : Les données de localisation sont des informations qui indiquent la position géographique ou l'emplacement physique d'un appareil, d'une personne ou d'un objet.
- **Hypertrucage** : L'hypertrucage fait référence à la manipulation de contenu média (souvent audio ou vidéo) à l'aide d'outils d'intelligence artificielle (IA) pour leur donner une apparence réaliste alors que ce contenu est fictif.
- **Paramètres de sécurité** : Les paramètres de sécurité sont des options ou des contrôles configurables au sein de divers appareils, applications, plateformes ou systèmes qui permettent aux utilisateurs de personnaliser et d'améliorer les mesures de sécurité en fonction de leurs préférences et de leurs besoins.
- **Compte ou profil public** : Un compte public est un compte dont le contenu et les informations sont visibles par tout le monde, sans posséder de compte ou de contact direct avec le profil.
- **Compte ou profil privé** : Un compte privé est un compte qui ne permet qu'à des personnes sélectionnées, généralement les amis ou les personnes qui suivent l'utilisateur, d'avoir accès au contenu qu'il partage.

- **Fuite de données** : Une fuite de données se produit lorsque des informations sensibles ou confidentielles sont divulguées involontairement ou malicieusement à des personnes ou entités non autorisées.
- **Intelligence artificielle** : L'intelligence artificielle (IA) est le développement de systèmes informatiques ou de logiciels capables d'effectuer des tâches qui requièrent généralement l'intelligence humaine, comme l'apprentissage, le raisonnement, la résolution de problèmes, la compréhension du langage naturel, la reconnaissance vocale et la perception visuelle.
- **Piratage** : Au sens général, le piratage informatique désigne l'obtention d'un accès non autorisé à des systèmes ou réseaux informatiques, impliquant souvent la manipulation, l'exploration ou l'exploitation de la technologie pour atteindre cet objectif.
- **Fraude** : La fraude est la tromperie intentionnelle ou la déformation des faits dans le but d'obtenir un avantage injuste ou malhonnête, souvent à des fins financières. Elle implique l'utilisation de pratiques trompeuses pour amener des individus, des organisations ou des systèmes à croire ou à agir sur la base de fausses informations.

Balayez ce QR code à l'aide de votre caméra pour visionner nos vidéos