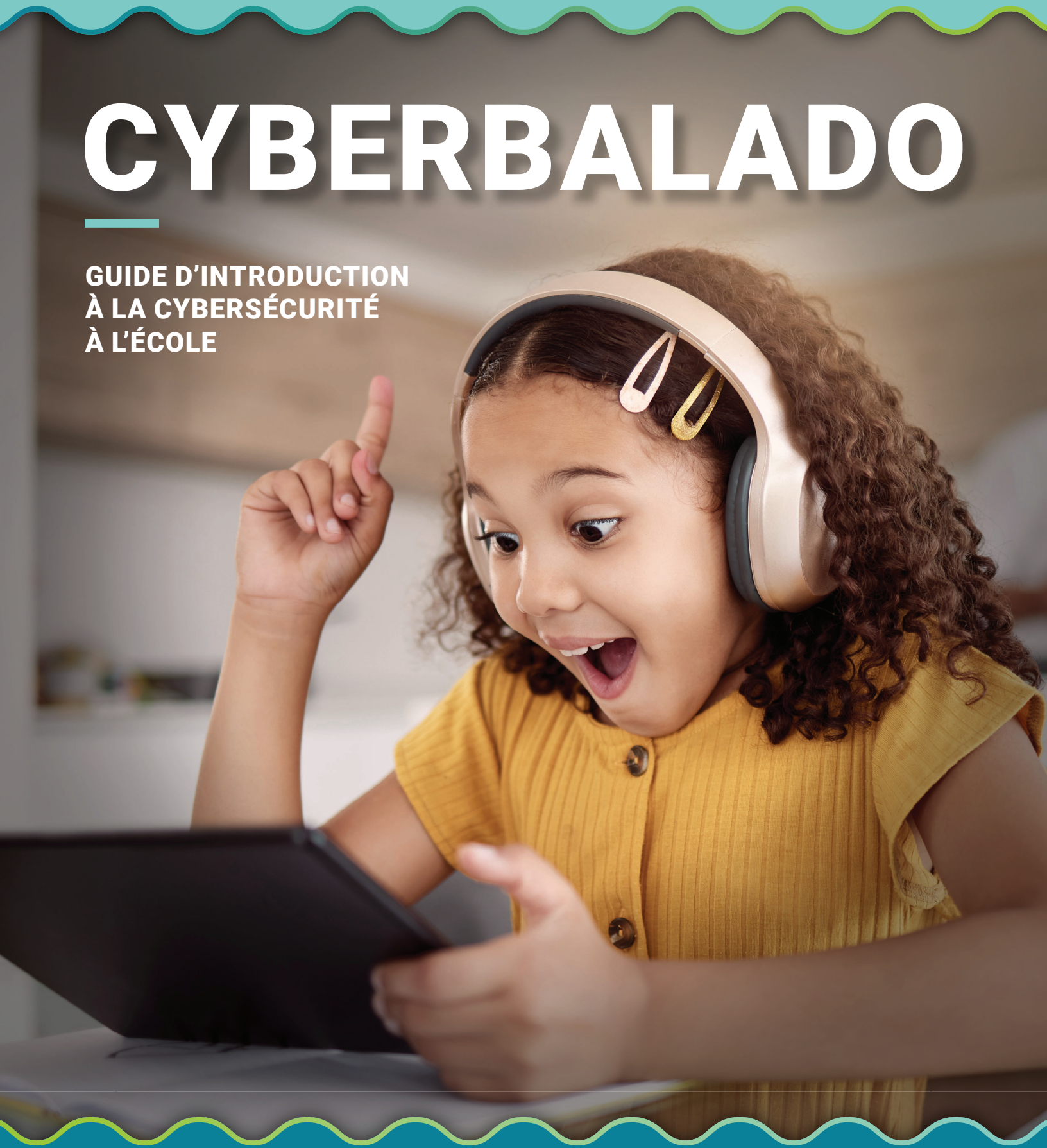
CYBERBALADO

GUIDE D'INTRODUCTION À LA CYBERSÉCURITÉ À L'ÉCOLE



CYBER BALADO

net good PAR cira

idée éducation entrepreneuriale

Ce guide a été réalisé grâce à la contribution financière de l'Autorité canadienne pour les enregistrements Internet (CIRA) dans le cadre du Programme de financement de Subventions Net Good de CIRA.

Le CIRA est une organisation nationale à but non lucratif qui est avant tout connue pour le rôle qu'elle joue dans la gestion du domaine .CA au nom de la population canadienne. Étant une organisation à but non lucratif formée de membres, CIRA a pour objectif de bâtir un Internet fiable pour les Canadien·nes.

ISBN à venir

AUTEURS:
Patrick Pierard, Idée éducation entrepreneuriale
Jean-Sébastien Reid, Idée éducation entrepreneuriale
Valérie Touchette, Idée éducation entrepreneuriale

VALIDATION DES CONTENUS :
Roberto Gauvin, Édunovis

GRAPHISME:
Ariane Thibault, Graphiste, Impression Novalie

RÉVISION LINGUISTIQUE:
Patrick Pierard

Édition de décembre 2024

IDÉE ÉDUCATION ENTREPRENEURIALE
www.idee.education
1566, rue de Zermatt, Sainte-Adèle (Qc) Canada J8B 2Z5
info@idee.education
1-877-930-4333

Merci de vous approprier la lecture en choisissant le pronom qui vous convient

TABLE DES MATIÈRES

INTRODUCTION ET MISE EN CONTEXTE 5

DÉFINITION DE LA CYBERSÉCURITÉ 6

POURQUOI EST-CE IMPORTANT? 6

LES RELATIONS ENTRE L'ÉDUCATION ENTREPRENEURIALE CONSCIENTE ET LA CYBERSÉCURITÉ 8

LES GRANDS PRINCIPES DE LA CYBERSÉCURITÉ 12

LES DIFFÉRENTS SUJETS DE LA CYBERSÉCURITÉ 14

- Mots de passe 15
- Mise à jour des logiciels 17
- Sécurité des réseaux Wi-Fi 18
- Internet des objets 20

LES MENACES EN LIGNE 21

- Hameçonnage (ou phishing) 22
- Cyberintimidation 23
- Sites non sécurisés 2
- Fausses nouvelles 27
- Validité des sources 28

L'UTILISATION RESPONSABLE D'INTERNET 32

- Réseaux sociaux 33
- Jeux en ligne 35
- Paramètres et politiques de confidentialité 36
- Achats en ligne 38
- Respect des droits d'auteur 40

L'INTELLIGENCE ARTIFICIELLE 41

CONCLUSION 45

- Références pour aller plus loin 45

ANNEXE : ACHATS EN LIGNE LISTE DE VÉRIFICATION 47

INTRODUCTION

MISE EN CONTEXTE

INTRODUCTION

MISE EN CONTEXTE

Un nombre important de jeunes canadiens du primaire et du secondaire restent vulnérables aux dangers liés à l'utilisation d'Internet. Plusieurs éducateurs et enseignants du niveau primaire et secondaire, ne maitrisent pas la cybersécurité ce qui les rend vulnérables dans l'utilisation de l'Internet et d'outils numériques dans un cadre pédagogique. Idée éducation entrepreneuriale souhaite, grâce au projet CyberBalado, développer leurs habiletés, en les formant à une utilisation sécuritaire de l'Internet grâce à une série de baladodiffusions accompagnées d'une trousse pédagogique.

Ce projet de baladodiffusion est un nouvel outil de sensibilisation et d'éducation pour gérer les risques des activités en ligne des jeunes en abordant des thématiques telles que la cyberintimidation, les techniques d'hameçonnage, les logiciels malveillants, le piratage, la mésinformation, etc. Les baladodiffusions seront cocréées et animées par des classes de jeunes de divers groupes d'âge entre 5 et 18 ans, soutenus par des pédagogues expérimentés.

Nous souhaitons permettre ainsi aux jeunes d'agir en visionnaires et leaders responsables en discutant des sujets qui les touchent. Notre équipe de pédagogues animera des ateliers dans les classes afin de permettre aux jeunes présents d'entreprendre et de s'entreprendre grâce à la baladodiffusion.

Le projet est rendu possible grâce au financement « NetGoods » du CIRA, l'Autorité canadienne pour les enregistrements Internet. Voici comment le CIRA décrit son programme : « Le programme Net Good par CIRA se base sur la prémisse selon laquelle Internet constitue un net avantage pour le monde. Nous soutenons des projets, des collectivités et des politiques qui améliorent l'Internet pour l'ensemble de la population canadienne. Pour ce faire, nous nous appuyons sur trois piliers : l'infrastructure, la sécurité en ligne et l'engagement politique. Nous versons également des subventions pour les initiatives Internet communautaires, par le biais d'un appel à candidatures annuel. Nous collaborons avec des partenaires dans les secteurs de la technologie et de la politique, à l'échelle nationale et internationale.

Le programme Net Good par CIRA est financé par les revenus que nous générons grâce aux domaines .CA et aux services de cybersécurité. »[1]

[1] https://www.cira.ca/fr/net-good/

DÉFINITION DE LA CYBERSÉCURITÉ

POURQUOI EST-CE IMPORTANT?

DÉFINITION DE LA CYBERSÉCURITÉ

Selon CyberCap, la cybersécurité englobe toutes les actions entreprises pour assurer la confidentialité, l'intégrité et la disponibilité des informations et des systèmes informatiques. Son objectif principal est de prévenir et de détecter les cyberattaques, telles que le piratage, le vol de données, les logiciels malveillants, etc.

De plus, l'organisme canadien Sécurité publique Canada affirme que le Gouvernement du Canada veut appuyer le développement et augmenter le niveau de cybersécurité de base au Canada. On peut y lire : « Des particuliers qui utilisent quelques technologies aux férus de technologie qui sont fermement ancrés dans le monde virtuels, nombreux ne savent pas qu'ils peuvent être visés par des cybermenaces. Par conséquent, ils ne prennent aucune mesure pour se protéger contre les cyberincidents et se rétablir le cas échéant. Même ceux qui sont conscients de l'importance de protéger leurs renseignements trouvent difficile de mettre en place des mesures abordables et efficaces. »[2]

POURQUOI EST-CE IMPORTANT?

Les enjeux de cybersécurité, font partie de nos conversations de plus en plus régulièrement. Nous avons tous un proche qui a reçu un courriel frauduleux ou encore un message qui lui demande de modifier son mot de passe soi-disant compromis.

Néanmoins, si on questionne les personnes de notre entourage, elles en connaissent très peu sur la cybersécurité. Il nous parait donc essentiel de contribuer à créer dans nos milieux scolaires des contextes où les jeunes prendront en charge la responsabilité d'informer, sensibiliser, rassurer et collaborer à une utilisation plus sécuritaire de l'Internet.

[2] https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-fr.aspx#s52

LES RELATIONS ENTRE L'ÉDUCATION ENTREPRENEURIALE CONSCIENTE ET LA CYBERSÉCURITÉ

La philosophie derrière l'éducation entrepreneuriale consciente[3] repose sur deux piliers incontournables :

1. Le développement de la personne et
2. Le développement à portée sociale

[3] https://idee.education/fr/notre-modele/philosophie/

En résumé on souhaite que les jeunes dans nos écoles puissent agir dès maintenant afin d'influencer positivement leurs communautés. Ils sont des agents de changement qu'on oublie trop souvent de mettre en action. Notre rôle est de leur donner les outils et les stratégies afin qu'ils puissent initier, réaliser et gérer des initiatives entrepreneuriales qui feront que notre monde sera meilleur grâce à leur contribution.

Profil de sortie

École communautaire entrepreneuriale consciente

Compétences
S'entreprendre, Entreprendre, Créer l'innovation de façon consciente, responsable et autonome

Attitudes
Fierté identitaire et culturelle, Recherche constante d'innovation, Engagement communautaire

Qualités
Confiance en soi, Curiosité, Créativité, Respect des autres, Esprit d'équipe, Sens de l'organisation, Solidarité, Sens des responsabilités, Sens de l'initiative, Ingéniosité, Leadership, Conscience entrepreneuriale, Apprentissage autonome, Empathie

Forces 3D
Diagnostic, Dynamisme, Détermination

Rôles
Initiateur, Réalisateur et Gestionnaire de projets

Toutes ces expériences se traduisent par le développement d'un profil de sortie en éducation entrepreneuriale consciente sur lequel on retrouve des cibles éducatives qui permettent aux intervenants scolaires de suivre l'évolution individuelle des jeunes de leurs groupes.

Il est intéressant de faire les liens entre le profil de sortie et les comportements à adopter dans un contexte de cybersécurité en débutant par les qualités entrepreneuriales conscientes.

LA CONFIANCE EN SOI

Souvent l'inconnu ou le manque de confiance crée des inquiétudes et de la peur. L'Internet est une source inépuisable de découvertes et il faut apprendre à naviguer avec confiance en sachant éviter les pièges. Néanmoins, un excès de confiance peut aussi nous faire baisser la garde et ne pas prendre au sérieux certaines menaces ou certaines failles.

LA CURIOSITÉ

Avoir le goût de découvrir de nouvelles choses et comprendre le fonctionnement des systèmes peuvent nous permettre de mieux percevoir les pièges ou les failles auxquels nous pourrions être confrontés. Vouloir se maintenir informés des nouvelles tendances et des nouvelles compétences à développer contribue à se protéger également.

La curiosité peut aussi nous jouer de mauvais tours. Par exemple, nous faire ouvrir des liens envoyés dans des courriels frauduleux ou des demandes qui nous font prendre des décisions trop rapides. Les cyberpirates trouvent des moyens pour nous faire réagir rapidement sans qu'on prenne assez de temps pour réfléchir. Ils vont par exemple nous faire croire que nous avons gagné un prix ou qu'il faut transmettre des informations personnelles rapidement. Il faut rester très prudent.

LA CRÉATIVITÉ

Voir la cybersécurité comme une forme de défi à travers lequel grandir plutôt qu'une contrainte à éviter permet de trouver de nouvelles manières de bien vivre avec les réalités de la cybersécurité.

RESPECT DES AUTRES, ESPRIT D'ÉQUIPE, SOLIDARITÉ ET EMPATHIE

Il est important de s'ouvrir aux autres lorsqu'il est question de sécurité en ligne et de questionner notre entourage. Ensemble, on peut ainsi évaluer les risques et trouver des solutions aux questions rencontrées. Il faut également développer notre écoute et notre empathie envers les personnes plus démunies de nos communautés. L'univers numérique est souvent perçu comme difficile à saisir pour ces personnes vulnérables.

Il est essentiel de demander de l'aide et de vérifier auprès d'adultes de confiance au besoin. Il est plus facile d'agir avant plutôt qu'après avoir été victime d'une cyberattaque. Si vous hésitez à prendre une décision, parlez-en à un adulte de confiance au lieu d'espérer que tout sera correct. En discuter avec d'autres est une action essentielle en cybersécurité.

SENS DES RESPONSABILITÉS

Nous avons tous la responsabilité de partager nos connaissances et compétences afin que nos communautés soient plus sécuritaires et mieux sensibilisées. Il faut que nos jeunes soient vigilants et ouverts à prendre en charge une part de la responsabilité d'éduquer à la cybersécurité. Leur voix aura sans doute une portée plus proche de leurs réalités que celle des adultes.

INITIATIVE ET APPRENTISSAGE AUTONOME

L'adoption de bonnes pratiques en cybersécurité revient au départ à chaque individu, mais en groupe on peut certainement aller plus loin. Néanmoins, en développant soi-même son autonomie numérique et en souhaitant apprendre pour la vie (mentalité de croissance), nous avons de meilleures chances d'avoir du succès dans le domaine de la cybersécurité, un domaine en constant changement.

LEADERSHIP

Les jeunes dans nos communautés sont des leaders qu'on doit mettre en lumière. Leur volonté à vouloir changer les choses inspirera leurs proches et la communauté qui les entoure. Les jeunes sont des acteurs de changements!

INITIATEUR RÉALISATEUR GESTIONNAIRE

Ces trois rôles sont fondamentaux dans l'émergence des cibles du profil de sortie. Nous croyons que si nous permettons aux jeunes de joueur progressivement ces rôles dans la classe, ils nous épateront par leurs idées et leur énergie. Osons oser leur faire confiance et croire en leur potentiel.

La relation entre la cybersécurité et le profil de sortie est inspirée du texte de Nicolas-Loïc Fortin paru dans l'École branchée, Volume 27, numéro 1 (automne 2024)[4]

[4] https://ecolebranchee.com/cybersecurite-enjeu-humain-ere-numerique/

LES GRANDS PRINCIPES DE LA CYBERSÉCURITÉ

Comme vous avez pu le constater dans la section précédente, nous croyons que l'humain derrière la cybersécurité joue un rôle majeur et incontournable.

VOICI 7 PRINCIPES DE BASE EN CYBERSÉCURITÉ À TOUJOURS METTRE EN PRATIQUE :

1.

S'INFORMER
... pour en savoir toujours plus sur l'actualité numérique
... pour adapter notre comportement aux nouvelles connaissances

2.

ADOPTER DE BONNES PRATIQUES
... pour éviter les erreurs ou les comportements à risque
... pour qu'elles deviennent des réflexes

3.

FAIRE PREUVE DE VIGILANCE
... pour avoir toujours l'œil aux aguets
... pour éviter d'être impulsif

4.

APPRENDRE TOUTE NOTRE VIE
... pour apprendre à réagir et être proactif
... pour comprendre le fonctionnement de ce qu'on utilise

5.

DÉVELOPPER NOS HABILETÉS SOCIO-ÉMOTIONNELLES
... pour gérer notre anxiété
... pour développer notre empathie
... pour faire preuve de solidarité

6.

FAIRE PREUVE DE JUGEMENT CRITIQUE
... pour faire des choix judicieux sur ce que nous consultons ou publions sur Internet et sur les réseaux sociaux

7.

DÉVELOPPER NOTRE FLAIR NUMÉRIQUE
... pour mieux repérer les fraudes, les pièges ou les fausses nouvelles
... pour mieux évaluer les risques que nous rencontrons

LES DIFFÉRENTS SUJETS DE LA CYBERSÉCURITÉ

Les fondamentaux de la cybersécurité

MOTS DE PASSE

Qu'est-ce qu'un mot de passe? C'est une combinaison de lettres, de chiffres et de caractères spéciaux comme «!@#$%??&&**()». Les mots de passe doivent être longs, 16 caractères ou plus. Ils sont choisis pour sécuriser un compte ou un appareil.

Un mot de passe, c'est comme une clé qui ouvre une porte ou la garde fermée pour ceux qui ne possèdent pas cette clé.

Les mots de passe protègent nos appareils, nos informations et nos comptes contre les intrusions : la porte reste fermée si le mot de passe est robuste.

Les mots de passe protègent ce que nous avons de plus importants : nos renseignements personnels, nos identités, notre argent et notre vie privée.

Un mot de passe facile à mémoriser est un mot de passe facile à deviner.

Il ne faut JAMAIS partager nos mots de passe avec nos amis ou pire, les écrire et les mettre en évidence près de nos appareils. Il est essentiel d'avoir des mots de passe différents selon nos activités : réseaux sociaux, école, banque, sites de divertissement, jeux en ligne, etc. Si un cyberpirate trouve votre mot de passe, il se peut qu'il essaie de l'utiliser sur d'autres comptes qui vous appartiennent.

Comment se protéger ?

- ✓ Utiliser des mots de passe robustes : longs, forts et uniques;
- ✓ Les changer tous les six mois;
- ✓ Utiliser au minimum 16 caractères et plus[5];
- ✓ Utiliser une combinaison de lettres majuscules et minuscules, de chiffres et de « caractères spéciaux » comme !@#$%?&*();
- ✓ Utiliser des paroles de chansons, des mots dans une autre langue ou des titres de films peu connus;
- ✓ Utiliser des phrases de passe composées d'au moins quatre mots choisis au hasard auxquels on ajoute quelques chiffres et signes. Ex. Fauteuil plante grue béton - 5plAnte%(gruebÉton?fauTeuil;
- ✓ Créer une phrase complète, prendre les premières lettres de chaque mot en majuscule ou en minuscule auxquelles on ajoute quelques chiffres et signes. Ex. Vendredi c'est l'halloween, j'ai bien hâte de manger des bonbons – vcLHja+$bh17DMdb4!;
- ✓ S'assurer de bien se déconnecter après chaque session;
- ✓ Utiliser l'authentification à deux étapes lorsque possible: oblige une seconde authentification après celle avec le mot de passe. (SMS, courriel, logiciel d'authentification, etc.). Ajoute donc une sécurité supplémentaire à vos informations importantes;
- ✓ Utiliser un gestionnaire de mot de passe : utile pour stocker vos différents mots de passe. Certains servent aussi à en générer de nouveaux, plus robustes. Le gestionnaire s'ouvre avec un seul mot de passe. Il en existe en ligne ou directement sur votre appareil. Il n'est pas recommandé d'y déposer les mots de passe trop sensibles par exemple celui de votre compte en banque.

Éléments à retenir

- ✓ Ne pas utiliser le même mot de passe pour tous ses comptes;
- ✓ Ne pas utiliser votre adresse, vos numéros de téléphone, des noms de votre famille et de vos animaux de compagnie;
- ✓ Ne pas utiliser des dates de naissance;
- ✓ Ne pas utiliser des mots de passe trop facile comme "123456" ou "motdepasse";
- ✓ Ne pas ajouter un chiffre ou une lettre au dernier mot de passe que vous aviez. Créez quelque chose de nouveau;
- ✓ Ne pas partager ses mots de passe même avec des personnes de confiance.

Les cyberpirates utilisent des dictionnaires de mot de passe qui contiennent la liste des mots de passe les plus courants ou qui ont déjà été piratés. Il est important que vos mots de passe soient uniques. Si vous croyez avoir été victime d'une attaque, il faut changer les mots de passe rapidement. Évitez à tout prix d'utiliser vos anciens mots de passe.

POUR EN SAVOIR PLUS

Votre mot de passe est-il suffisamment robuste ? Voici cinq façons de l'évaluer

https://www.pensezcybersecurite.gc.ca/fr/blogues/votre-mot-de-passe-est-il-suffisamment-robuste-voici-cinq-facons-de-levaluer

Bien, très bien, encore mieux : comment avoir un mot de passe plus robuste

https://www.pensezcybersecurite.gc.ca/fr/blogues/bien-tres-bien-encore-mieux-comment-avoir-un-mot-de-passe-plus-robuste

[5] https://cadre21.org/blogue/ressources/se-premunir-contre-les-cyberpirates/

MISE À JOUR DES LOGICIELS

Nos appareils numériques que ce soit un ordinateur, un téléphone, une tablette ou un appareil connecté ont besoin de mises à jour régulières. Certaines de ces mises à jour servent à améliorer ou à ajouter des fonctionnalités (mise à jour de version), mais certaines permettent aussi de corriger des failles de sécurité (mise à jour critique ou importante).

Les cybercriminels apprécient particulièrement trouver des failles sur ces appareils puisqu'ils renferment une foule de données associées à nos habitudes de vie sur Internet. Ils peuvent voir nos informations personnelles et financières, accéder à nos contacts, etc. Il est donc essentiel de colmater ces failles lorsqu'elles se présentent.

POUR EN SAVOIR PLUS

Pensez Cybersécurité
https://www.pensezcybersecurite.gc.ca/fr/blogues/mises-jour-logicielles-pourquoi-elles-sont-essentielles-pour-votre-cybersecurite

Pourquoi et comment bien gérer ses mises à jour ?
https://monurl.ca/misesajour

Pour y parvenir nous recommandons de maintenir vos appareils à jour. Voici quelques conseils:

1.

IDENTIFIER TOUS VOS APPAREILS À RISQUE

En créant cet inventaire vous vous assurez de mettre en place une procédure qui limite vos oublis et les risques de failles.

2.

ACTIVER LA MISE À JOUR AUTOMATIQUE

De cette manière, vous ne passerez pas à côté d'une mise à jour importante qui pourrait avoir un impact sur votre cybersécurité. On vous recommande de faire ces mises à jour lors de vos périodes d'inactivité afin de ne pas modifier le fonctionnement de vos appareils pendant que vous les utilisez.

3.

ASSUREZ-VOUS DE FAIRE LES MISES À JOUR À PARTIR DES SITES OFFICIELS

Certains cybercriminels reproduisent un environnement qui vous laisse croire que leur version de la mise à jour est la bonne. Il s'agit alors d'un cheval de Troie intéressant pour pénétrer dans vos appareils.

4.

PROTÉGEZ VOS APPAREILS VIEILLISSANTS

Si vous avez un appareil qui n'est pas (ou n'est plus) en mesure de recevoir des mises à jour, vous devrez être encore plus prudent. Nous vous conseillons de fermer les fonctionnalités plus risquées ou de le retirer de votre réseau d'appareils.

SÉCURITÉ DES RÉSEAUX WI-FI

LES RÉSEAUX WIFI PRIVÉS

Presque tout le monde au Canada a un réseau wifi à la maison. Il permet de brancher nos appareils à Internet par l'intermédiaire d'un routeur ou d'un modem généralement fourni par la compagnie avec laquelle on fait affaire. Le réseau wifi privé doit être bien protégé pour éviter le piratage des données ou des appareils ainsi que le branchement et l'utilisation illégaux de notre connexion internet privée à des fins criminelles. Le propriétaire peut être tenu criminellement responsable de l'utilisation de son réseau privé.

Que faire ?

- ✓ Modifier les réglages par défaut du routeur, le nom et le mot de passe;
- ✓ Utiliser une phrase de passe solide et difficile à deviner (voir section sur les mots de passe);
- ✓ Dans la mesure du possible, placer le routeur au centre de la maison pour limiter la portée du réseau wifi privé.

LES RÉSEAUX WIFI PUBLICS

S'ils peuvent être pratiques parfois, ils ne sont en général pas protégés. Ce qui place les usagers dans une situation à hauts risques : piratage, installation de logiciel malveillant, faux points d'accès, etc.

Que faire ou pas ?

- ✓ Désactiver le wifi si vous n'utilisez pas Internet;
- ✓ Faire régulièrement les mises à jour des logiciels (particulièrement le système d'exploitation et le coupe-feu);
- ✓ Activer ou installer un coupe-feu qui vérifiera la conformité de tout autre appareil qui tente d'accéder au vôtre par Internet;
- ✓ Ne jamais accéder à vos renseignements financiers, magasiner en ligne ou prendre vos messages à partir d'un réseau wifi public.

SÉCURITÉ DES RÉSEAUX WI-FI

LE BLUETOOTH

La technologie Bluetooth est bien pratique lorsqu'il s'agit de connecter des écouteurs ou des haut-parleurs à nos appareils. Cependant, il faut savoir qu'un Bluetooth activé dans un endroit public est une porte d'entrée parfaite pour les pirates de toutes sortes. Si une personne peut détecter votre appareil par Bluetooth, elle pourra aussi le pirater. Lorsque la fonction Bluetooth est activée, l'adresse de votre appareil est visible sur tous les appareils Bluetooth de l'environnement immédiat.

Que faire ?

- ✓ Désactiver votre signal Bluetooth surtout dans les endroits publics;
- ✓ Ne jamais se connecter au Bluetooth de personnes inconnues ou en qui on n'a pas confiance;
- ✓ Si un des appareils Bluetooth est inutilisé, perdu ou volé, il faut immédiatement le retirer de la liste des appareils associés à votre téléphone ou ordinateur.

L'UTILISATION D'UN RÉSEAU PRIVÉ VIRTUEL (RPV OU VPN EN ANGLAIS)

Un RPV est une connexion sécurisée qui sert de tunnel protecteur entre votre appareil et Internet. Un RPV peut assurer que toutes vos données sont sécurisées et chiffrées avant de se retrouver sur Internet.

L'utilisation d'un RPV est particulièrement recommandée si vous êtes connecté à un réseau wifi public.

POUR EN SAVOIR PLUS

La sécurité du Wi-Fi (ITSP.80.002) - Centre canadien pour la cybersécurité
https://www.cyber.gc.ca/fr/orientation/la-securite-du-wi-fi-itsp80002

Sécurisez vos connexions – Pensez Cybersécurité
https://www.pensezcybersecurite.gc.ca/fr/securisez-vos-connexions

INTERNET DES OBJETS
(IDO OU INTERNET OF THINGS (IOT), EN ANGLAIS)

UNE DÉFINITION RAPIDE

Nous utilisons de plus en plus d'objets connectés à Internet. Ils sont pratiques, par exemple, pour contrôler certains appareils à distance. On peut penser aux multiples caméras de surveillance, aux dispositifs pour contrôler les lumières ou encore la température de la maison. Ces dispositifs sont branchés sur Internet et permettent à nos appareils informatiques d'entrer en communication avec eux. Cela inclut aussi des jouets connectés via une application, des montres intelligentes qui suivent l'activité physique, envoient des messages et même parfois génèrent des appels d'urgence. Il y a aussi les assistants vocaux comme Alexa ou Google Home utilisés pour poser des questions, écouter de la musique ou contrôler d'autres appareils connectés. Le problème est que souvent, tous ces appareils peuvent aussi servir de porte d'entrée à des pirates informatiques.

De plus en plus de villes utilisent des objets connectés car cela facilite leur fonctionnement en général. Par exemple, pour le contrôle des lumières et de la température dans les édifices municipaux. On parle alors de villes intelligentes et celles-ci doivent aussi utiliser les outils de la cybersécurité pour se protéger.

POURQUOI EST-CE IMPORTANT EN CYBERSÉCURITÉ ?

Les objets connectés sont une porte d'entrée pour les pirates informatique. C'est un peu comme si nous laissions une fenêtre ouverte à la maison. Les pirates informatiques essaient de trouver toutes les issues possibles. Malheureusement, certains objets connectés ne sont pas bien sécurisés et utilisent des mots de passe trop simples. Cela permet aux pirates informatiques d'accéder à des réseaux ainsi qu'à des données et à des informations personnelles.

Certains objets connectés nous arrivent dans leur emballage original avec un mot de passe simple par défaut (par exemple "0000"). Les fabriquants font ceci pour que ce soit plus facile lors de la fabrication. Par contre, il est très important de remplacer ces mots de passe simples par des mots de passe plus robustes. Plusieurs pirates informatiques utilisent des dictionnaires de mots de passe qui les aident à déjouer la sécurité d'objets connectés et ainsi accéder à un réseau et à des données personnelles.

La règle à privilégier avec les objets connectés

Lorsqu'on utilise un objet connecté, il est essentiel de s'assurer que cet objet puisse être sécurisé par un mot de passe robuste. C'est aussi une bonne idée de prendre un temps d'arrêt et de réfléchir sur l'importance ou non d'utiliser certains objets connectés. Nous devons avoir le réflexe de privilégier le côté sécuritaire plutôt que le côté pratique.

POUR EN SAVOIR PLUS

Radio-Canada | Doit-on craindre les objets connectés ? | Article de presse ;
https://ici.radio-canada.ca/nouvelle/1430274/objets-connectes-intelligents-enceinte--dangereux-danger-enregistre-vie-privee-donnees

Le Figaro | Un casino piraté à cause d'un thermomètre d'aquarium ; Lien et source de l'article 1 | Article de presse ;
https://www.lefigaro.fr/secteur/high-tech/2018/04/16/32001-20180416ARTFIG00278-un-casino-pirate-a-cause-d-un-thermometre-dans-un-aquarium.php

SI TU VEUX DÉCOUVRIR L'UNIVERS DES VILLES INTELLIGENTES

Demain la ville | La smart city est morte, vive la smart city! | Vidéo YouTube ;
https://www.youtube.com/watch?v=WEB9nmfPsv8

LES MENACES EN LIGNE

HAMEÇONNAGE (OU PHISHING)

Généralement l'hameçonnage se pratique à partir de courriels ou de messages texte qui sont envoyés à un grand nombre de personnes par des fraudeurs dans l'espoir que certains mordent à l'hameçon.

POUR EN SAVOIR PLUS

Que faire d'un message qui vous semble suspect ?

https://www.pensezcybersecurite.gc.ca/fr/ressources/que-faire-dun-message-qui-vous-semble-suspect

COMMENT RECONNAÎTRE UN COURRIEL OU UN MESSAGE TEXTE D'HAMEÇONNAGE ?

- **Il y a souvent une notion d'urgence.** L'auteur veut que le destinataire réponde très rapidement, il peut y avoir des menaces de fermeture de compte ou de poursuites.
- **Des informations sensibles vous sont demandées.** Les institutions ne demandent jamais de fournir des renseignements personnels par courriel ou texto.
- **Il ne faut jamais cliquer sur des liens** vers des pages d'ouverture de session.
- **Il faut se méfier** :
  - Des demandes de mise à jour des renseignements associés à vos comptes;
  - Des demandes de renseignements financiers, même s'ils semblent provenir de banques ou de fournisseurs de services avec lesquels vous faites affaire;
  - Des concours auxquels vous n'avez jamais participé;
  - Des prix pour lesquels il faut débourser une somme d'argent;
  - Des héritages de lointains parents;
  - Des reçus ou des suivis d'envoi pour des articles que vous n'avez pas commandés;
  - Des remboursements desquels vous n'êtes pas au courant;
  - Tout autre sujet qui paraît bizarre.
- **Il est possible de reconnaître les tentatives d'hameçonnage** à certaines caractéristiques :
  - Des courriels provenant d'adresses qui imitent des adresses légitimes;
  - Des logos mal imités;
  - Des fautes d'orthographe ou de grammaire;
  - Des pièces jointes suspectes.
- Quand on n'est pas certain de l'origine de ce que l'on a reçu, **les précautions suivantes s'imposent :**
  - Ne pas cliquer sur les liens;
  - Ne pas répondre ni transférer le message;
  - Ne jamais ouvrir les pièces jointes;
  - Supprimer le courriel ou le message texte.
- Si des doutes subsistent, on peut contacter le présumé émetteur par téléphone pour vérifier la validité du courriel ou du message texte.
- **Les relations affectives virtuelles cachent souvent des fraudeurs.** Après des mois d'une relation affective virtuelle qui est appréciée (échange de photos, mots doux, gentillesse, sans jamais se rencontrer), la personne a soudain un besoin financier très pressant pour une raison plausible : problème de santé, voyage urgent, dette à rembourser, aide d'un membre de la famille, etc. Si vous prêtez de l'argent dans de telles conditions, il y a de fortes chances que vous ne les revoyez plus jamais : ni l'argent, ni la personne.

CYBERINTIMIDATION

DÉFINITION

On parle de cyberintimidation quand une personne en intimide une autre en utilisant un moyen technologique: réseaux sociaux, sites Web, messageries (courriels, textos), etc.

Le cyberharcèlement est un synonyme de cyberintimidation.

POUR EN SAVOIR PLUS

Cyberintimidation : les gestes interdits | Éducaloi
https://educaloi.qc.ca/capsules/cyberintimidation-les-gestes-interdits/

DES EXEMPLES

POUR LES ENFANTS, LES ADOLESCENTS ET LES ADULTES

- Envoyer un grand nombre de messages blessants à quelqu'un;
- Ridiculiser quelqu'un sur les réseaux sociaux ;
- Nuire à la réputation d'une personne en publiant quelque chose qui pousserait les gens à la haïr, la mépriser ou la trouver ridicule;
- Formuler des insultes graves contre quelqu'un;
- Menacer quelqu'un de sévices physiques ou matériels;
- Menacer pour obtenir quelque chose d'une personne (extorsion);
- Propager des secrets ou des rumeurs sur la personne.

POUR LES ADOLESCENTS ET LES ADULTES

- Créer de faux comptes sur les médias sociaux pour ridiculiser quelqu'un;
- Enregistrer une personne à son insu et diffuser cet enregistrement sur les médias sociaux;
- Publier les photos intimes de quelqu'un sans son autorisation ou menacer de le faire en échange d'argent ou d'autre matériel intime (sextorsion);
- Inciter une personne à se faire du mal ou à se suicider.

Plusieurs des exemples mentionnés ici sont des comportements réprimés par la loi. Ils peuvent faire l'objet de plaintes à la police et conduire à des verdicts de culpabilité.

POUR EN SAVOIR PLUS

C'est quoi le cyberharcèlement ?
https://www.e-junior.fr/module/le-cyberharcelement

CYBERINTIMIDATION

CARACTÉRISTIQUES DE LA CYBERINTIMIDATION

- Les actes de cyberintimidation se propagent très rapidement;
- Le contenu peut atteindre de très nombreuses personnes;
- La technologie permet aux cyberintimidateurs(-trices) de se cacher facilement;
- Par sa nature virtuelle, la cyberintimidation peut être plus compliquée à faire cesser;
- Il est très difficile de faire supprimer le contenu une fois publié en ligne;

CONSÉQUENCES

Les jeunes qui sont victimes de cyberintimidation ressentent de nombreuses émotions négatives : humiliation, confusion, peur, sentiment d'isolement, honte, perte d'estime de soi, culpabilité.

QUE FAIRE SI JE SUIS VICTIME DE CYBERINTIMIDATION ?

Dans un premier temps :

- Éviter de réagir impulsivement;
- Garder des traces des gestes de cyberintimidation : captures d'écran, enregistrements, messages, etc.;
- Bloquer les personnes qui harcèlent.

Dans un second temps :

- Trouver un adulte de confiance à qui en parler : parent, ami, professeur, etc.;
- Prévenir la direction de l'école de la situation vécue;
- Prévenir la police si la cyberintimidation transgresse la loi (il serait préférable d'avoir des conseils à ce sujet d'une personne de confiance);
- Consulter un médecin ou un psychologique si la cyberintimidation cause des perturbations de la santé physique et/ou mentale.

CYBERINTIMIDATION

PRÉVENTION

Les conseils suivants ne garantissent pas un environnement exempt d'intimidation. Cependant ces bonnes habitudes sont un premier pas vers la sécurité en ligne.

- Garder les mots de passe confidentiels, même avec les personnes très proches;
- Maîtriser les paramètres de confidentialité et les fonctions de signalement sur les médias sociaux;
- Toujours bien réfléchir avant de publier ou de partager du contenu personnel ou des informations sensibles sur les réseaux sociaux;
- Bloquer les personnes malveillantes ou qui publient des éléments qui mettent mal à l'aise.

POUR EN SAVOIR PLUS

Aidez moi SVP

https://needhelpnow.ca/fr/#trouver-de-l-aide

Jeunesse j'écoute

https://jeunessejecoute.ca/information/cyberintimidation-definition-et-solutions/

SITES NON SÉCURISÉS

COMMENT LES RECONNAÎTRE ET S'EN PROTÉGER

Naviguer sur Internet peut être risqué si l'on ne fait pas attention. Savoir reconnaître les sites sécurisés est crucial pour protéger vos informations.

QU'EST-CE QU'UN SITE SÉCURISÉ ?

Un site sécurisé est un site qui commence par "https://" et un petit cadenas est présent dans la barre d'adresse de votre navigateur. Cela signifie que vos informations sont protégées.

QUELS SONT LES RISQUES DE NAVIGUER SUR UN SITE NON SÉCURISÉ ?

VOL D'INFORMATIONS : Vos données personnelles peuvent être compromises.

MALWARE : Des logiciels malveillants peuvent infecter vos appareils.

VOICI QUELQUES CONSEILS POUR NAVIGUER EN TOUTE SÉCURITÉ:

- ✓ Cherchez le cadenas dans la barre d'adresse et s'assurer que le l'adresse URL commence par "https";
- ✓ Ne partagez pas d'informations personnelles telles que votre nom, adresse ou numéro de téléphone sur des sites non sécurisés;
- ✓ Utilisez un pseudonyme;
- ✓ Vous pouvez aussi naviguer en mode privé afin de masquer vos informations personnelles et votre adresse IP (identifier et géolocaliser votre ordinateur).
- ✓ Installer un logiciel antivirus pour détecter, identifier et supprimer les logiciels malveillants et les fichiers suspects.

POUR EN SAVOIR PLUS

Sécurisez vos connexions – Pensez Cybersécurité https://www.pensezcybersecurite.gc.ca/fr/securisez-vos-connexions

Pensez Cybersécurité https://www.pensezcybersecurite.gc.ca/fr

FAUSSES NOUVELLES

DES BUTS DIFFÉRENTS

- **LA MÉSINFORMATION :** diffuser de la fausse information sans avoir de mauvaises intentions.
- **LA DÉSINFORMATION :** diffuser de la fausse information dans le but de manipuler ou de tromper des personnes, des organisations et des États ou bien de leur faire du tort.
- **LA MALINFORMATION :** diffuser de l'information qui repose sur un fait, mais qui est souvent exagérée de façon à tromper ou même à causer des préjudices.

Quoi vérifier pour s'assurer que la nouvelle est fiable ?

Parmi les bonnes pratiques à adopter, la capacité de jugement critique s'applique à tous les domaines de la cybersécurité. Pour détecter les fausses nouvelles en ligne et en comprendre les mécanismes sous-jacents, une bonne réflexion sera nécessaire à chaque occasion. Douter sera votre meilleur atout.

Comment valider la source d'un article?

On recommande de faire le recensement de trois sources d'informations différentes sur le même sujet. Vous verrez ainsi si votre nouvelle est validée ou si elle est contredite par d'autres sources par ce principe de triangulation.

VOICI LES INGRÉDIENTS D'UNE INFORMATION FIABLE PUBLIÉE EN LIGNE :

- ✓ La source est bien identifiée : il s'agit d'un média reconnu;
- ✓ L'article est accompagné d'une image en lien direct avec le sujet et correctement décrite;
- ✓ Il y a un titre, une date de parution et la signature du (de la) journaliste;
- ✓ L'article est coiffé d'un chapeau (aussi appelé lead) : un premier paragraphe souvent en caractères gras qui fournit un résumé de l'information qui suit.

VOICI LES RÉFLEXES QU'IL FAUT DÉVELOPPER FACE À UNE NOUVELLE SUSPECTE :

- ✓ Consulter un site de vérification des faits pour déterminer si l'information a déjà été réfutée;
- ✓ Lancer une recherche d'image inversée pour connaître la provenance d'une photo et sa véracité;
- ✓ Ne pas tenir pour acquis que l'information que vous recevez est correcte, même si elle provient d'une source que l'on juge valide (comme un ami ou un proche).

POUR EN SAVOIR PLUS

Centre québécois d'éducation aux médias et à l'information : guides pédagogiques https://www.cqemi.org/fr/outils-pedagogiques

Fausses nouvelles, les repérer et les déjouer - BANQ https://www.banq.qc.ca/notre-institution/grande-bibliotheque/fausses-nouvelles-les-reperer-et-les-dejouer/

Les as de l'info https://lesasdelinfo.com/

Habilomédias https://habilomedias.ca/

Hoaxbuster - La plateforme collaborative contre la désinformation https://www.hoaxbuster.com/

Comment enseigner aux élèves à détecter les fausses nouvelles ? https://www.edcan.ca/articles/teach-students-identify-fake-news/?lang=fr

VALIDITÉ DES SOURCES

COMMENT RECONNAÎTRE UN SITE D'INFORMATION FIABLE

Aujourd'hui Internet est rempli d'informations provenant de diverses sources: journaux en ligne, réseaux sociaux comme Discord et TikTok, blogs, médias alternatifs, YouTubeurs et influenceurs. Tout le monde peut publier sur le web. Avec autant de sources disponibles, il peut être difficile de distinguer les informations fiables des informations douteuses.

C'est donc dire que les informations que nous trouvons en ligne peuvent être bonnes, mauvaises, vraies, fausses, ou exagérées. Pour bien s'informer, que ce soit pour un projet scolaire ou pour rester à jour avec les dernières nouvelles, il est essentiel de savoir reconnaitre et identifier les sites fiables et ceux à éviter.

POURQUOI EST-CE IMPORTANT ?

Éviter la désinformation :

En apprenant à identifier les sources fiables, vous pouvez éviter de propager des informations incorrectes ou trompeuses.

Prendre des décisions éclairées:

Des informations précises et fiables vous aident à prendre des décisions basées sur des informations justes et variées au quotidien.

Développer une pensée critique :

Savoir évaluer la fiabilité des sources renforce votre capacité à analyser et à critiquer les informations que vous recevez. À distinguer un point de vue versus un fait, et plus encore.

VALIDITÉ DES SOURCES

QU'EST-CE QU'UNE SOURCE D'INFORMATION FIABLE ?

Une source d'information fiable est une source qui fournit des informations exactes, vérifiées, objectives et pertinentes sur un sujet donné. Pour évaluer la fiabilité d'une source d'information, il faut prendre en compte plusieurs critères par exemple :

L'AUTEUR.	**QUI** est l'auteur de la source ? L'auteur est-il un expert dans son domaine ? Quelles sont ses qualifications, ses compétences, son expérience, sa crédibilité, son objectivité ?
LA DATE.	**QUAND** la source a-t-elle été publiée ou mise à jour ? Est-elle récente ou date-t-elle de plusieurs années ?
LE CONTENU.	**DE QUOI** est-il question ? Quel est le contenu de la source ? Quelles sont les informations, les données, les faits, les arguments, les opinions, les analyses, les interprétations, les commentaires, les résumés, etc.
LA SOURCE.	**D'OÙ** proviennent les informations, les données, les faits, les opinions ? Le site appartient-il à une organisation reconnue ? Les informations sont-elles citées, référencées, sourcées, vérifiées, validées ?
LE BUT.	Quel est le but/l'objectif de la source ? Quelle est son intention, son message, son contexte, son point de vue, son biais, son intérêt ?
LA FORME.	Quelle est sa présentation, son style, son ton, sa clarté, sa cohérence ?

VALIDITÉ DES SOURCES

QU'EST-CE QU'UNE SOURCE D'INFORMATION FIABLE ?

Voici un aide-mémoire que nous avons créé dans notre plateforme "J'ai une idée" :

Qui est l'auteur ? Recherche l'auteur de l'information. Est-ce une personne ou une organisation respectée dans le domaine ?

De quoi est-til question ? L'information est-elle pertinente pour le sujet de ma recherche ? Est-elle exacte et confirmée par au moins deux autres ressources ?

D'où provient l'information ? La source cite-t-elle ses informations ? Les sources citées sont-elles également fiables ?

De quand date la publication ? Les informations sont-elles récentes ou mises à jour régulièrement ?

Pourquoi est publiée l'information ? La source présente-t-elle l'information de manière objective ?

Comment est présentée l'information ? Est-ce que l'information est claire, présentée de manière professionnelle, sans fautes d'orthographe ou de grammaire ?

Ne pas hésiter à consulter plusieurs sources. Consulter plusieurs sources peut vous aider à avoir une meilleure compréhension d'un sujet en obtenant des perspectives différentes.

Utiliser des sources d'information variées. Ceci fait référence à l'utilisation de plusieurs types de sources pour obtenir une vue complète et équilibrée d'un sujet. Cela inclut des articles, des livres, des vidéos, des interviews, et bien plus encore. En comparant les informations provenant de différentes sources, vous pouvez vérifier leur exactitude et éviter les biais.

VALIDITÉ DES SOURCES

VOICI QUELQUES EXEMPLES DE SOURCES FIABLES:

1. **LIVRES PÉDAGOGIQUES:**
   Publiés pas des maisons d'éditions reconnues;

2. **JOURNAUX SCIENTIFIQUES:**
   Publient des articles écrits par les pairs;

3. **SITES WEB GOUVERNEMENTAUX:**
   Fournissent souvent des statistiques et des rapports officiels;

4. **MÉDIAS DE CONFIANCE:**
   Des organisations médiatiques réputées pour leur journalisme précis et impartial.

En suivant ces conseils, vous serez mieux équipés pour naviguer dans l'univers de l'information en ligne et trouver des sources fiables pour vos recherches et vos sources d'informations.

POUR EN SAVOIR PLUS

La crédibilité des sites internet | Alloprof
https://www.alloprof.qc.ca/fr/eleves/bv/francais/la-credibilite-des-sites-internet-f1415

Comment reconnaître un site d'information fiable - École branchée
https://ecolebranchee.com/scoop/infodemie-ou-comment-reconnaitre-un-site-dinformation-fiable/

L'UTILISATION RESPONSABLE D'INTERNET

RÉSEAUX SOCIAUX

RÉPUTATION EN LIGNE

Votre réputation en ligne, c'est ce que les gens pensent de vous en ligne. On y retrouve les contenus que vous créez, publiez et partagez, et la nature de vos interactions avec les autres.

Ce que les autres créent, publient et partagent sur vous fait aussi partie de votre réputation en ligne. La plupart du temps, ces contenus sont publics. Même s'ils sont privés, ils peuvent devenir publics rapidement, notamment par capture d'écran.

Les personnes que vous suivez ou avec qui vous interagissez en ligne donnent également une image de vous.

La façon la plus simple de découvrir la réputation en ligne de quelqu'un est de rentrer son nom dans un moteur de recherche. Ce qui apparaîtra permettra rapidement de se forger une idée de qui est la personne. Même si une telle recherche est très superficielle, elle n'en constitue pas moins un premier contact qui peut parfois être déterminant. Ce peut être de nouveaux amis, des écoles et même de futurs employeurs qui vérifient la réputation en ligne des personnes. Ne jamais oublier que tout ce qui se trouve en ligne y reste pour longtemps sinon pour toujours. Des éléments publiés il y a plusieurs années peuvent resurgir à tout moment.

D'où l'importance de bien maîtriser les paramètres de confidentialité des différents réseaux sociaux et jeux que vous utilisez.

RÉSEAUX SOCIAUX

Parmi les réseaux sociaux les plus connus, on trouve Tiktok, Facebook, Instagram, Snapchat, X, YouTube, etc. Ils peuvent être un moyen pratique de partager des contenus (photos, événements, renseignements, etc.) avec des amis ou de la famille. Là comme ailleurs, certains dangers guettent les usagers de ces plateformes si populaires.

Selon le type de partage que l'on veut faire, il faut choisir le réseau social qui semble le mieux répondre à nos valeurs et à nos intentions : se faire connaître, partager avec des amis ou la famille, apprendre, éduquer, s'informer, aider, faire de la publicité, etc. Avant d'ouvrir un compte, il faut se demander si c'est un outil qui correspond bien à notre personnalité.

L'âge minimal requis pour ouvrir un compte sur la majorité des réseaux sociaux est fixé à 13 ans. De très nombreux jeunes s'y retrouvent dès l'âge de 11 ou 12 ans. Certains états ont légiféré sur ce sujet et mis en place des mécanismes de validation de l'âge. Au Canada, aucune loi n'encadre l'âge d'accès aux réseaux sociaux.

RÉSEAUX SOCIAUX

POUR EN SAVOIR PLUS

Grandir en ligne : Qu'est-ce qui se cache derrière mes réseaux sociaux ? - MAJ - Radio-Canada
https://ici.radio-canada.ca/jeunesse/maj/2114897/documentaire-impact-adolescents-cerveau-medias

De meilleurs réseaux sociaux s'en viennent - La Presse
https://www.lapresse.ca/affaires/techno/2024-09-22/de-meilleurs-reseaux-sociaux-s-en-viennent.php

PRINCIPAUX DANGERS DES RÉSEAUX SOCIAUX

Les réseaux sociaux ont plusieurs avantages. Nous sommes nombreux à le reconnaître. D'après les dernières estimations, ce sont plus de 5 milliards de personnes en 2023 qui ont utilisé les réseaux sociaux soit plus de 62% de la population mondiale. C'est dire que quand vous utilisez les réseaux sociaux, vous n'êtes pas seuls. Cette immense popularité vient avec son lot de malveillance ou de risques. En tant qu'utilisateur responsable, vous vous devez d'agir.

VOICI QUELQUES DANGERS ET LES FAÇONS DE LES DÉJOUER :

CYBERHARCÈLEMENT : Dépasser la peur. Ne pas s'isoler. Aller chercher de l'aide auprès des adultes. En discuter avec son entourage et porter plainte au média social et éventuellement à la police. (Voir la section sur la cyberintimidation)

USURPATION D'IDENTITÉ : Changer les mots de passe régulièrement. Réagir en cas d'activité suspecte. Rentrer régulièrement son nom sur les moteurs de recherche pour vérifier que personne n'a usurpé votre identité. Vérifier souvent vos profils pour s'assurer que rien n'a été publié sans votre autorisation. Rester attentif à toute activité ou commentaire suspects de la part d'autres utilisateurs.

ARNAQUE : Concours trop facile, message de gains faramineux, propositions irréalistes etc. sont en général des signes de fraudes. Éviter de répondre, de cliquer sur des liens inconnus et plus généralement d'entrer en contact avec les expéditeurs. (Voir la section sur l'hameçonnage)

PIRATAGE : Ne jamais publier de données personnelles sur les réseaux sociaux. Protéger vos comptes en activant les paramètres de sécurité. S'assurer que seules les personnes que vous choisissez puissent accéder à votre profil.

AMI(E) VRAIMENT ? : Refuser les demandes « d'amis » de personnes que vous ne connaissez pas bien ou pas du tout. Bloquer les personnes qui envoient des messages qui mettent mal à l'aise.

CHALLENGES VIRAUX : Si certains challenges présentés sur les réseaux sociaux peuvent s'avérer utiles, la majorité peuvent mettre en danger la vie ou la santé des utilisateurs. À éviter.

MISE EN DANGER DE LA RÉPUTATION EN LIGNE : Toujours bien réfléchir avant de publier en ligne, éviter les publications impulsives et les débats d'opinions. Ne jamais poster de contenu irrespectueux ou offensant. Une fois en ligne, votre publication ne disparaitra jamais.

PARTAGE DE FAUSSES INFORMATIONS : Éviter de repartager de l'information sans en avoir validé les sources. (Voir la section sur les sources fiables)

RISQUES POUR LA SANTÉ : Être conscient que les réseaux sociaux ne reflètent pas la réalité, être capable de prendre du recul. Limiter le temps passé sur les réseaux sociaux chaque jour. Pratiquer des activités autres qu'en ligne.

MÉCANISMES DE SIGNALEMENT : les réseaux sociaux possèdent tous aujourd'hui des mécanismes qui permettent de signaler des contenus ou comportements inappropriés. Ne jamais hésiter à les utiliser.

COMPTES FICTIFS : les comptes fictifs ne publient pas beaucoup de contenu, mais essaient de faire partie de nos réseaux. En acceptant ces comptes, vous leur donnez accès à vos listes d'amis, à vos publications et à certaines de vos informations personnelles. Des robots de l'IA sont utilisés pour créer de faux profils sur les réseaux sociaux. Par exemple sur X, de plus en plus de faux profils essaient d'inciter les gens à investir de l'argent dans certaines cryptomonnaie ou autre.

JEUX EN LIGNE

Les jeux en ligne sont devenus une activité très populaire, offrant des univers fascinants où l'on peut explorer de nouveaux mondes, rencontrer d'autres joueurs et vivre des aventures exaltantes. Mais derrière ces mondes virtuels se cachent des enjeux de sécurité.

POURQUOI LA CYBERSÉCURITÉ EST ESSENTIELLE DANS LES JEUX EN LIGNE ?

PROTECTION DES DONNÉES PERSONNELLES : Lorsque vous créez un compte sur un jeu en ligne, vous fournissez des informations personnelles qui peuvent être utilisées à mauvais escient si elles ne sont pas protégées correctement.

RISQUES DE PIRATAGE ET D'USURPATION D'IDENTITÉ : Les comptes de jeu peuvent être piratés, ce qui permet aux pirates d'accéder à vos informations personnelles.

CYBERHARCÈLEMENT : Certains joueurs peuvent être méchants ou intimidants.

INTERACTIONS AVEC DES INCONNUS: Partager des informations personnelles peut être dangereux. Ou encore avoir des conversations sur des sites de clavardage avec certains joueurs dont vous ne connaissez pas la réelle identité.

CONSEIL POUR JOUER EN TOUTE SÉCURITÉ

- ✓ Utilisez des pseudonymes;
- ✓ Vérifiez les paramètres de confidentialité et veillez à comprendre les politiques de confidentialité du site ou les autorisations que vous acceptez. Configurez les options de confidentialité et fermez les comptes que vous n'utilisez plus;
- ✓ Faites attention aux liens suspects et aux endroits où vous cliquez. Il peut apparaitre des fenêtres de publicités ou autre selon le site que vous utilisez;
- ✓ Faites attention aux personnes que vous rencontrez en ligne dans les jeux vidéo. Lorsque vous jouez en ligne, il est important de garder à l'esprit que les personnes que vous rencontrez ne sont pas toujours celles qu'elles prétendent être. Certains joueurs peuvent créer de faux profils pour tromper les autres, il est possible que ces personnes ne soient même pas réelles.

POUR EN SAVOIR PLUS

Cyberaide.ca

Game mentor https://lementor.gg/

Comment gérer les dépenses en jeu : Guide pour les parents | Questions Internet ? https://www.internetmatters.org/fr/resources/online-money-management-guide/in-game-spending-tips-to-support-young-people/

PARAMÈTRES ET POLITIQUES DE CONFIDENTIALITÉ

Imaginez que toutes vos conversations privées, même les plus personnelles dans Messenger ou Discord, soient projetées sur un écran géant et que tout le monde puisse les lire. Pour éviter cela, il est essentiel de bien comprendre et maîtriser les paramètres de confidentialité de vos comptes en ligne.

QU'EST-CE QU'UN PARAMÈTRE DE CONFIDENTIALITÉ ?

C'est un réglage qui vous permet de choisir qui peut voir les informations que vous partagez en ligne. C'est un peu comme un cadenas que vous posez sur votre porte pour protéger votre intimité.

POURQUOI EST-CE IMPORTANT ?

PROTÉGEZ VOTRE VIE PRIVÉE : vous décidez qui peut voir vos photos, vos vidéos, vos messages et vos informations personnelles. Sur certains sites comme Facebook, vous décidez également qui peut publier du contenu sur votre page et vous pouvez également choisir d'approuver le contenu avant qu'il soit publié. D'autres paramètres comme « bloquer un commentaire ou un ami » sont également possibles. Activer des paramètres comme ceux-ci vous permet de contrôler les contenus qui façonnent en partie votre identité numérique et dans certains cas peut éviter des publications de cyberintimidation.

COMMENT RÉGLER VOS PARAMÈTRES DE CONFIDENTIALITÉ ?

PRENEZ LE TEMPS DE LIRE LES POLITIQUES DE CONFIDENTIALITÉ lorsque vous ouvrez un compte et avant d'accepter. Il est vrai qu'il peut être ennuyeux de prendre le temps de le faire, et il vous est sûrement arrivé d'accepter sans en prendre connaissance. Cependant, la politique de confidentialité d'un site, d'un jeu ou d'une application que vous téléchargez constitue une forme de contrat que nous signons virtuellement

SOYEZ SÉLECTIFS DANS LE CHOIX DE VOS AMI(E)S EN LIGNE. Acceptez uniquement les demandes d'ami(e)s de personnes que vous connaissez dans la vraie vie.

LIMITEZ LA VISIBILITÉ DE VOS PUBLICATIONS. Choisissez qui peut voir vos publications: tous (toutes) vos ami(e)s, seulement vos proches ou des personnes spécifiques seulement.

ADAPTEZ VOS PARAMÈTRES DE CONFIDENTIALITÉ AU BESOIN. Les paramètres peuvent changer et certains paramètres peuvent être appliqués pour certains contenus. Voici un exemple avec Facebook : vous pourriez publier une vidéo que vous avez enregistrée lors d'une activité en famille et la partager avec elle seulement et non pas avec tous (toutes) vos ami(e)s.

PARAMÈTRES ET POLITIQUES DE CONFIDENTIALITÉ

LES POLITIQUES DE CONFIDENTIALITÉ C'EST QUOI ?

Les politiques de confidentialité sont des documents essentiels qui expliquent comment une entreprise ou un service en ligne collecte, utilise et protège nos données personnelles. Il est donc crucial de prendre le temps de les lire afin de comprendre ce que nous acceptons concernant nos informations et l'utilisation qui en est faite par l'entreprise. Par exemple, nos coordonnées peuvent être utilisées par des agences de marketing pour promouvoir des produits.

Dans certaines politiques de confidentialité, en cliquant sur "Acceptez", nous consentons à ce que tout ce que nous publions, y compris nos photos personnelles, devienne public et que le site en ait l'usage. Des exemples courants sont Facebook et Instagram qui stipulent que les contenus partagés peuvent être visibles par d'autres utilisateurs et utilisés par la plateforme à des fins de publicité ou de promotion.

VOICI QUELQUES CONSEILS SUPPLÉMENTAIRES:

- ✓ Ne partagez pas d'informations personnelles sensibles en ligne. Évitez de publier vos coordonnées ou encore, selon le contexte, évitez d'indiquer où vous êtes à un moment précis.
- ✓ Méfiez-vous des demandes d'informations personnelles inattendues. Les politiques de confidentialité vous aident à identifier ces tentatives d'hameçonnage en vous informant des pratiques légitimes de l'entreprise ou de la manière dont elle communiquera avec vous.
- ✓ Informez-vous lors des mises à jour de politiques de confidentialité d'une organisation.

POUR EN SAVOIR PLUS

Office de protection du consommateur (Québec) https://www.opc.gouv.qc.ca/consommateur/sujet/renseignements-personnels/

10 conseils à suivre pour protéger vos renseignements personnels – Commissariat à la protection de la vie privée du Canada https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-et-conseils-pour-les-particuliers/votre-droit-a-la-vie-privee/02_05_d_64_tips/

ACHATS EN LIGNE

PAIEMENTS SÉCURISÉS, PROTECTION DES DONNÉES.

L'achat en ligne a complètement transformé notre façon de consommer. Aujourd'hui les adultes achètent des vêtements, des livres et profitent des meilleures offres disponibles sur Internet. C'est pourquoi il est important de recevoir des conseils pour naviguer en toute sécurité dans le monde des achats en ligne.

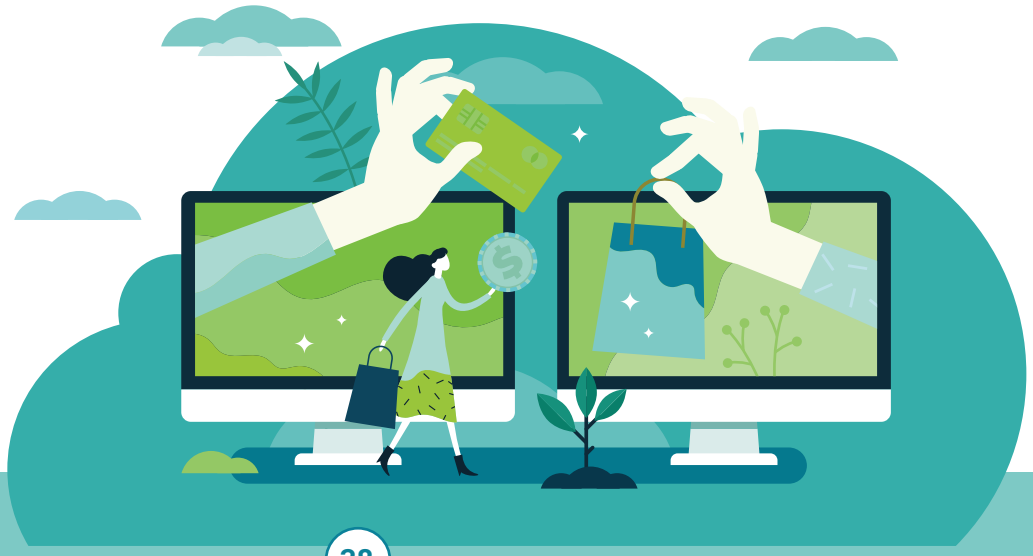
POURQUOI L'ACHAT EN LIGNE EST-IL POPULAIRE?

L'achat en ligne est pratique et souvent plus rapide que de se rendre en magasin. Parfois, le produit que nous souhaitons acheter n'est pas disponible en magasin ou est uniquement disponible en ligne. On peut comparer les prix, lire les avis et trouver des produits partout sur la planète sans quitter notre domicile.

LES RISQUES D'ACHAT EN LIGNE

Bien que l'achat en ligne soit de plus en plus présent au quotidien, il comporte des risques. Nos informations personnelles et financières peuvent être en danger si on ne fait pas attention.

Dans un premier temps, il est important de reconnaitre les sites sécurisés, de comprendre l'importance des mots de passe forts, d'éviter de laisser nos comptes connectés sur les appareils que nous utilisons (objets connectés) et de se méfier des offres trop belles pour être vraies ou de piètre qualité. On peut aussi se questionner sur la qualité de notre achat, le service après-vente, l'option d'échange et de retour si notre achat ne convient pas.



ACHATS EN LIGNE

CONSEILS POUR DES ACHATS EN LIGNE SÉCURISÉS :

Voici quelques conseils afin de faire des achats en ligne sécurisés :

- ✓ **UTILISER DES SITES INTERNET SÉCURISÉS :** Voir la section sur les sites non sécurisés.
- ✓ **PROTÉGER VOS INFORMATIONS PERSONNELLES :** Ne partagez jamais vos informations personnelles ou bancaires sur des sites non sécurisés.
- ✓ **S'ASSURER DE SE DÉCONNECTER :** Selon l'appareil utilisé, qu'il soit personnel, partagé ou public, il est important de toujours se déconnecter de son compte après l'utilisation. De plus, il ne faut jamais sauvegarder ses mots de passe sur ces appareils ni même sur nos appareils personnels pour éviter que d'autres personnes y accèdent.
- ✓ **CRÉER DES MOTS DE PASSE FORTS :** Voir la section sur les mots de passe
- ✓ **VÉRIFIER LES AVIS ET LES ÉVALUATIONS :** Lisez les avis des autres acheteurs pour vous assurer de la fiabilité du vendeur. Si vous ne connaissez pas l'entreprise, effectuez une recherche pour en savoir plus et vérifiez qu'il s'agit d'une compagnie fiable. Cela peut inclure la consultation de leur site internet officiel, la vérification de leur présence sur les réseaux sociaux et la recherche de mentions ou d'articles à leur sujet.
- ✓ **ÉVITER LES OFFRES TROP ALLÉCHANTES :** Si une offre semble trop belle pour "être vraie", elle l'est possiblement.
- ✓ **ÉVITER DE SE LAISSER INFLUENCER PAR LES OFFRES FRÉQUENTES :** Pour éviter les achats impulsifs, il est préférable de prendre son temps avant de finaliser un achat.

Voir la liste de vérification proposée en annexe. En prenant le temps de réfléchir, vous pourrez faire des choix plus judicieux et éviter les achats impulsifs.

POUR EN SAVOIR PLUS

Comment faire des achats en ligne en toute sécurité - Centre canadien pour la cybersécurité
https://www.cyber.gc.ca/fr/orientation/comment-faire-des-achats-en-ligne-en-toute-securite-itsap00071

Conseils de consommation : avant d'acheter par Internet – OPC Québec
https://www.opc.gouv.qc.ca/consommateur/sujet/achat/internet/conseils/

Pas certain si ce site d'achat en ligne est frauduleux ? Quelques outils pour vous aider. Ce guide fournit des conseils pratiques pour naviguer en toute sécurité sur Internet, y compris comment reconnaître les sites sécurisés et éviter les fraudes.
https://www.pensezcybersecurite.gc.ca/fr/blogues/pas-certain-si-ce-site-dachat-en-ligne-est-frauduleux-quelques-outils-pour-vous-aider

RESPECT DES DROITS D'AUTEUR

COPYRIGHT, LICENCES, PLAGIAT.

Il est vraiment facile de trouver des images, vidéos, œuvres numériques sur Internet, mais est-ce qu'on peut les utiliser comme bon nous semble ? Si nous sommes les créateur(-trice)s de ces œuvres, est-ce que tout le monde peut les utiliser ?

Généralement, nous ne pouvons pas utiliser la création d'une personne ou d'une organisation sans sa permission. De plus, si nous avons son autorisation, il est important de bien citer la source de la création afin que les lecteur(-trice)s ou auditeur(-trice)s de notre production sachent qui est à l'origine de l'œuvre initiale.

Nous vous conseillons de suivre ces règles afin de respecter la loi sur les droits d'auteur et le travail des créateur(-trice)s :

- ✓ Choisir des œuvres qui sont sur des banques libres de droits. C'est-à-dire que vous pouvez les utiliser pour votre propre publication. Il arrive toutefois qu'on vous demande d'inscrire la source de l'image.
- ✓ Utiliser des productions qui sont identifiées par une norme de partage internationale comme les « Creative commons ». Elle permet à l'auteur d'indiquer sous quelles conditions il accepte de partager sa création.
- ✓ Contacter directement le (la) créateur(-trice) afin de convenir de l'utilisation en tout ou en partie de l'œuvre que vous souhaitez utiliser.

POUR EN SAVOIR PLUS

Le droit d'auteur : quand utiliser l'œuvre de quelqu'un d'autre – Éducaloi
https://educaloi.qc.ca/capsules/droit-auteur-quand-utiliser-oeuvre/

Office de la propriété intellectuelle du Canada
https://ised-isde.canada.ca/site/office-propriete-intellectuelle-canada/fr/guide-droit-dauteur

L'INTELLIGENCE ARTIFICIELLE

L'INTELLIGENCE ARTIFICIELLE

Autant nous avons peur des impacts de l'émergence de l'intelligence artificielle que nous sommes renversés par ses immenses possibilités. Son expansion publique s'est beaucoup manifestée par l'arrivée de Chat GPT en 2022. À partir de ce moment, toute la puissance de l'intelligence artificielle apparaissait aux yeux du monde. Chaque requête nourrit cette intelligence. Elle devient toujours de plus en plus précise et efficace à chaque fois qu'un usager lui soumet une demande. Il importe donc de mettre en œuvre les principes de bases de la cybersécurité avec encore plus de rigueur afin de ne pas se faire piéger. Nous allons, ci-dessous, vous présenter quelques aspects de l'influence de l'intelligence artificielle sous l'angle de la cybersécurité avec quelques conseils pour se protéger.

LES DONNÉES PERSONNELLES ET L'IA

Il est important, tout comme pour les autres outils numériques, de faire preuve de la même prudence lorsque vous utilisez des applications de l'intelligence artificielle. Il faut éviter de divulguer ou de fournir vos informations personnelles puisqu'on ne maîtrise pas toujours ce que cet outil pourrait en faire et à qui il pourrait les partager.

Lorsque vous créez un compte sur un outil de l'IA, bien lire les conditions d'utilisation de vos données.

LES BIAIS DE L'IA

La programmation à l'origine des outils de l'IA combinée avec l'entraînement que ces IA suivent créent des biais dans les algorithmes. Lorsqu'on parle de biais, il s'agit d'une influence, parfois involontaire, générée par ses créateur(-trice)s et utilisateur(-trice)s et qui se retrouve à l'intérieur de la programmation de l'IA.

L'IA s'entraîne grâce aux requêtes des utilisateurs et à des ensembles de données tirés du web. Il arrive que ces éléments soient interprétés de façon erronée par l'IA parce qu'ils contiennent des erreurs ou que les données sont biaisées.

Ne jamais oublier que l'IA est une production humaine et qu'elle reflète les forces et les biais des personnes qui la bâtissent.

POUR EN SAVOIR PLUS

Qu'est-ce qu'un biais
https://monurl.ca/allaboutai

L'INTELLIGENCE ARTIFICIELLE

LES HYPERTRUCAGES DE L'IA

Il est possible et facile d'utiliser des applications afin « d'emprunter » la voix ou le visage d'une personne et d'en créer une forme de clone numérique. On appelle hypertrucage « le procédé de manipulation audiovisuelle qui recourt aux algorithmes de l'apprentissage profond pour créer des trucages ultraréalistes[6] ». Soyez très vigilant afin de ne pas tomber dans le piège qu'un cyberpirate pourrait vous tendre à propos de quelqu'un de votre entourage. Il est donc primordial, dès qu'on vous présente une vidéo d'un proche vous demandant de l'argent ou vous faisant croire quelque chose de peu crédible de contacter personnellement cette personne proche. Ainsi vous connaîtrez la vérité et peut-être éviterez-vous de poser un geste financier que vous regretteriez.

L'IA GÉNÉRATIVE

L'utilisation de l'IA générative (exemples : ChatGPT, Dalle-E, Copilot, Gemini, etc.) peut poser des problèmes quant au respect des droits d'auteur et à la protection des données personnelles. En effet, ce qui est produit par ces IA à partir des commandes soumises n'est pas nécessairement privé. Ainsi, le contenu peut circuler et ne respecte pas toujours les droits d'auteur. Toutefois, si vous soumettez une requête en déposant un élément pour lequel il y a des droits d'auteur (image, texte, etc.), vous devez vous assurer d'être propriétaire de ces droits.

De la même manière, il n'est pas recommandé d'intégrer des informations personnelles dans une requête formulée à ces IA puisque ces informations pourraient circuler ou être reprises par des organismes tiers.

POUR EN SAVOIR PLUS

L'utilisation pédagogique, éthique et légale de l'intelligence artificielle générative – Guide destiné au personnel enseignant – 2024-2025 – Éducation Québec https://cdn-contenu.quebec.ca/cdn-contenu/education/Numerique/Guide-utilisation-pedagogique-ethique-legale-IA-personnel-enseignant.pdf

Orientations pour l'intelligence artificielle générative dans l'éducation et la recherche - UNESCO Bibliothèque Numérique https://unesdoc.unesco.org/ark:/48223/pf0000389901

LES HALLUCINATIONS DE L'IA ET LA MÉSINFORMATION

Il faut faire attention et reconnaître les hallucinations de l'IA. Selon Wikipédia[7], une hallucination est une réponse fausse ou trompeuse qui est présentée comme un fait certain. Ce phénomène est appelé « hallucination » par analogie avec le phénomène de l'hallucination en psychologie humaine.

Cependant, une différence clé est que l'hallucination humaine est généralement associée à de fausses perceptions, alors qu'une hallucination d'IA est associée à des réponses ou des croyances injustifiées.

Il est donc recommandé de toujours valider par triangulation les informations retrouvées dans un énoncé créé par l'IA. Ainsi, en validant par des sources externes les informations fournies vous aurez davantage l'assurance d'utiliser les bonnes informations.

Des exemples pertinents ici : https://www.techopedia.com/fr/dictionnaire/hallucination-ai

POUR EN SAVOIR PLUS

L'IA et son fonctionnement : Pour mieux comprendre ses impacts et ses enjeux – OBVIA https://www.obvia.ca/sites/obvia.ca/files/ressources/DossiersThematiques4nov.pdf

Guide d'intégration de l'IA pour les écoles – Éducation Nouveau-Brunswick https://www2.gnb.ca/content/dam/gnb/Departments/ed/pdf/Publications/guide-integration-ia.pdf

[6] https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26552557/hypertrucage

[7] Hallucination (intelligence artificielle) — Wikipédia, page consultée le 14 novembre 2024

CONCLUSION

CONCLUSION

Nous espérons que grâce à ce guide vous pourrez naviguer avec plus d'assurance dans le monde de la cybersécurité. Néanmoins, plusieurs sujets n'ont pu être abordés dans cette édition. Nous vous laissons le soin, grâce à vos initiatives d'éducation entrepreneuriale, de vous documenter adéquatement et de sensibiliser votre communauté sur les sujets abordés dans ce guide et/ou sur les autres possibilités proposées ici comme les objets connectés, les villes intelligentes, le bien-être numérique, etc.

RÉFÉRENCES POUR ALLER PLUS LOIN

Références pour le personnel scolaire

- Programme Enfants avertis
  www.enfantsavertis.ca
  Et leurs fiches de prévention :
  Parents www.enfantsavertis.ca
- Pensez Cybersécurité .ca (Gouvernement du Canada)
  https://www.pensezcybersecurite.gc.ca/fr
- Office québécois de la langue française - Vocabulaire de la sécurité informatique
  https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/vocabulaire-securite-informatique.aspx
- Habilomédias : dossier sur la cybersécurité
  https://habilomedias.ca/littératie-numérique-et-éducation-aux-médias/enjeux-numériques/cybersécurité
- La section sur la cybersécurité de LabosCréatifs
  https://www.laboscreatifs.ca/cybersecurite
- Guide pratique de la cybersécurité et de la cyberdéfense de l'Organisation internationale de la francophonie
  https://drive.google.com/file/d/1QkVZ-RP3RApNr7t5kz7xr1fKWnS8F_LA/view
- Linux, le système d'exploitation des hackers
  https://www.laboscreatifs.ca/documents/cyber-securite/Introduction-aux-commandes-Linux-en-cybersecurite.pdf
- L'utilisation pédagogique, éthique et légale de l'intelligence artificielle générative – Guide destiné au personnel enseignant – 2024-2025
  https://cdn-contenu.quebec.ca/cdn-contenu/education/Numerique/Guide-utilisation-pedagogique-ethique-legale-IA-personnel-enseignant.pdf

- IA en classe
  https://iago.re/index.html
- Bienvenue dans le monde de la cybersécurité – École branchée
  https://ecolebranchee.com/bienvenue-monde-cybersecurite/
- Éducation à la cybersécurité – ministère de l'Éducation nationale (France)
  https://monurl.ca/cyberduationalefr
- Centre canadien pour la cybersécurité (Gouv. Canada)
  https://www.cyber.gc.ca/fr
- L'École des Réseaux Sociaux
  https://www.schoolofsocialnetworks.org/fr/
- Guide pour s'informer en ligne avec des sources fiables (Nellie Brière)
  https://www.nelliebriere.ca/guide_fr

Formations en ligne

- Agence nationale de la sécurité des systèmes d'information (ANSSI) | Le MOOC de l'ANSSI | Site web
  https://secnumacademie.gouv.fr/
- Cours sur la citoyenneté numérique et la sécurité (Google)
  https://skillshop.exceedlms.com/student/path/111753-cours-sur-la-citoyennete-numerique-et-la-securite
- Cours 623 : Introduction à la cybersécurité pour les professionnels et professionnelles de l'éducation (Gouv. Canada)
  https://www.cyber.gc.ca/fr/education-communaute/carrefour-apprentissage/cours/623-introduction-cybersecurite-professionnels-professionnelles-leducation
- Éduquer à la cybersécurité – Cadre21
  https://cadre21.org/badges/eduquer-a-la-cybersecurite-1-explorateur
- École Cybersécurité
  https://www.ecolecyber.ca/

Références pour les jeunes

- Liste de vidéos suggérées par Télé-Québec accompagnée par des idées d'activités en lien avec les comportements et la sécurité en ligne
  https://monurl.ca/listeteleqc
- Mon identité numérique (Récit ECR)
  https://ecr.recitdp.qc.ca/mon-identit%C3%A9-num%C3%A9rique
- CTRL-F (Civix)
  https://ctrl-f.ca/fr/
- Conseils et informations de sécurité sur Internet | Questions Internet ?
  https://www.internetmatters.org/fr/advice/
- Enfants et ados | CNIL ?
  https://www.cnil.fr/fr/thematiques/enfants-et-ados

CYBER BALADO

ANNEXE : ACHATS EN LIGNE

LISTE DE VÉRIFICATION

- ☐ Est-ce que j'en ai réellement besoin ?
- ☐ Est-ce que cet achat correspond à mes besoins ou pourrais-je trouver une option plus adaptée ?
- ☐ Est-ce que j'ai comparé les prix avec d'autres sites pour être sûr d'obtenir la meilleure offre ?
- ☐ Est-ce que j'ai lu les avis des autres acheteurs pour m'assurer de la qualité du produit ?
- ☐ Est-ce que j'ai vérifié si le site est sécurisé (https) avant de saisir mes informations personnelles ?
- ☐ Est-ce que j'ai vérifié avec mon entourage si ce produit est connu, si le prix est bon, etc. ? Est-ce que j'ai demandé l'avis à mon entourage ou à une personne de confiance avant de faire un achat ?
- ☐ Est-ce que cet achat rentre dans mon budget ou est-ce que je dépense plus que ce que je peux me permettre ?


CYBER
BALADO