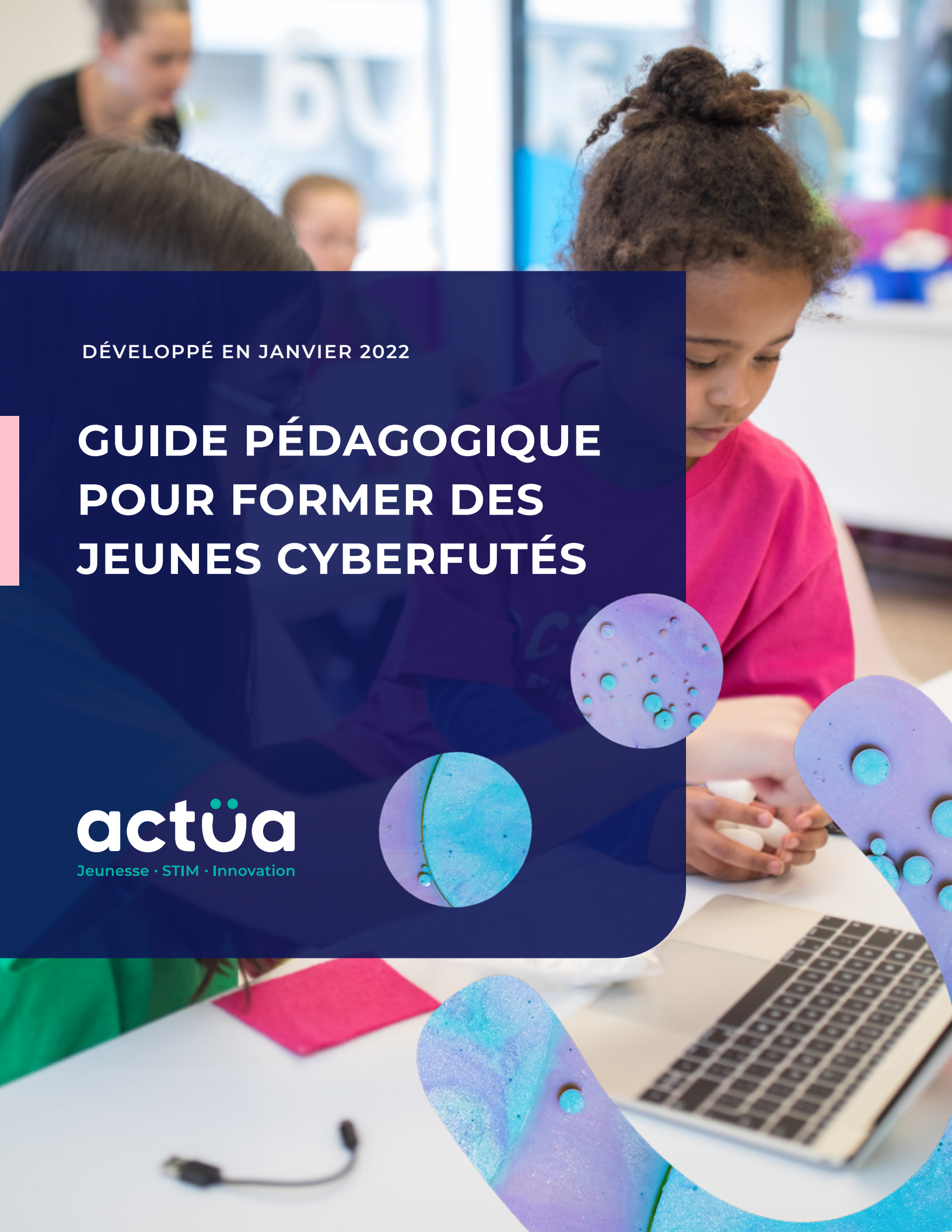


DÉVELOPPÉ EN JANVIER 2022

GUIDE PÉDAGOGIQUE POUR FORMER DES JEUNES CYBERFUTÉS

actüa

Jeunesse · STIM · Innovation

Table des matières

À propos d'Actua

Représentant plus de 40 universités et collèges à travers le pays, Actua est le principal réseau de sensibilisation des jeunes aux sciences, à la technologie, à l'ingénierie et aux mathématiques (STIM) au Canada.

Chaque année, 300 000 jeunes prennent part à des ateliers pratiques, à des camps et à des projets communautaires inspirants dans plus de 500 localités d'un océan à l'autre. Actua met l'accent sur la participation de jeunes sous-représentés dans le cadre de programmes destinés aux Autochtones, aux filles et aux jeunes femmes, aux jeunes à risque ainsi qu'à ceux vivant dans des communautés nordiques ou éloignées. Pour de plus amples renseignements, consultez notre site web à www.actua.ca et nos publications sur Twitter, Facebook, Instagram et YouTube!

Conditions D'utilisation

Mot de la PDG

Le monde virtuel constitue aujourd'hui un lieu accessible pour créer des liens, exprimer son opinion et développer un sentiment d'appartenance.

- JENNIFER FLANAGAN

Au Canada et dans le monde entier, la transformation numérique progresse à grands pas. Les jeunes fréquentent plus que jamais le cyberespace, comme ils ont dû utiliser des technologies comme l'ordinateur, la tablette ou le téléphone intelligent pour apprendre, communiquer et socialiser durant la pandémie de COVID-19. Pour plusieurs, le bouton Arrêt n'existe pas. Le monde virtuel constitue aujourd'hui un lieu accessible pour créer des liens, exprimer son opinion et développer un sentiment d'appartenance. Les interactions en ligne peuvent contribuer au développement sain et au bien-être des jeunes, mais elles les exposent aussi à diverses cybermenaces, comme l'hameçonnage, la fraude, le vol d'identité, l'intimidation et l'exploitation.

Dans le cadre de notre mission de libérer le potentiel infini des jeunes, nous travaillons sans relâche pour lever les obstacles à leur participation aux STIM. Parmi ces obstacles, on retrouve les cybermenaces et les cyberattaques, qui peuvent décourager les jeunes d'explorer, de créer et de communiquer en ligne. C'est pourquoi Actua estime que la cybersécurité et la citoyenneté numérique font partie de la littératie numérique et devraient être intégrées à tous les programmes de formation sur le sujet.

Le projet Mobilisation. Autonomisation. Connexion. (MAC) d'Actua vise à développer la cyberautonomie des jeunes par l'éducation à la citoyenneté numérique responsable

Nous voulons former une génération cyberfutée, prête à relever les défis de l'ère

numérique. Nous enseignons aux jeunes à poser un regard critique sur leurs interactions virtuelles, à éviter les dangers en ligne et à utiliser les technologies de manière innovante, saine et sûre. Nous aidons aussi les enseignantes et enseignants comme vous à initier leurs élèves aux pratiques cybersécuritaires. Le projet MAC est fondé sur le programme national d'Actua pour le développement des compétences numériques et en programmation. Cependant, nous y mettons à l'essai une nouvelle approche pour contrer les facteurs développementaux, socioéconomiques et technologiques qui rendent les jeunes, et en particulier les filles, plus vulnérables aux pressions sociales à l'œuvre sur Internet.

Nous vous invitons à vous joindre à nous et à notre réseau croissant de membres pour doter les jeunes des compétences, des connaissances et de l'assurance dont ils ont besoin pour devenir des citoyens numériques responsables et cyberfutés. Nous avons conçu le présent guide pour vous accompagner dans cette mission. Vous trouverez sur actua.ca d'autres renseignements, y compris des ressources et des activités pédagogiques sur la citoyenneté numérique, les pratiques cybersécuritaires et la cybersécurité.

Cordialement,

Jennifer Flanagan
Présidente et directrice générale d'Actua

Pourquoi et comment? (Par où commencer?)

Pourquoi avons-nous créé ce guide?

Nous vivons à l'ère numérique, une période où les technologies et Internet influencent grandement notre façon d'apprendre et de communiquer.

De nos jours, les enfants ont accès à une mine d'informations inépuisable. Selon Sécurité publique Canada, les moins de 25 ans passent en moyenne 7 heures en ligne chaque jour (La Sécurité au Canada, 2019). Ce chiffre peut surprendre lorsqu'on sait que 42 % des Canadiennes et Canadiens ont vécu au moins un cyberincident pendant la pandémie (Statistique Canada, 2020), ce qui met en évidence la hausse des cybermenaces et de leur complexité.

Si l'ère numérique offre une multitude de possibilités, elle présente aussi des enjeux et des risques qui peuvent avoir des effets négatifs sur les jeunes et leur entourage. Ce guide est l'un des volets du projet Mobilisation. Autonomisation. Connexion. (MAC) d'Actua, qui vise à fournir aux jeunes les connaissances, compétences et ressources nécessaires pour naviguer sur le web en toute sécurité. Ce projet aide les jeunes à :

- Devenir des citoyens numériques autonomes
- Créer des espaces positifs et inclusifs en ligne et hors ligne
- Prendre des décisions judicieuses et éclairées lors de l'utilisation des technologies
- Construire leur identité numérique activement et librement
- Adopter des pratiques cybersécuritaires pour résoudre leurs problèmes et atténuer les risques en ligne
- Reconnaître les partis pris médiatiques et la mésinformation
- Repérer et éviter diverses cybermenaces (hameçonnage, logiciels malveillants, etc.)

Comment utiliser ce guide?

Le présent guide est conçu pour vous aider à former des jeunes cyberfutés par l'enseignement de pratiques cybersécuritaires, de la cybersécurité et de la citoyenneté numérique. Vous y trouverez des points de vue d'expertes et d'experts et des notions de base qui faciliteront

l'animation des activités de la série MAC en classe. Grâce à ce guide, vous pourrez :

- Améliorer votre connaissance des principaux aspects de la vie numérique et de la cybersécurité (identités en ligne, citoyenneté numérique, stratégies de prévention, cybermenaces, etc.)
- Comprendre comment ces sujets peuvent s'inscrire dans le programme pédagogique de la maternelle à la 12e année et dans la vie réelle
- Parler de vie numérique et de cybersécurité à vos élèves au moyen d'une approche constructive et d'un langage valorisant
- Connaître les meilleures pratiques à adopter pour animer les activités de la série MAC
- Parfaire votre connaissance du vocabulaire entourant Internet, la cybersécurité et la citoyenneté numérique

Il n'est pas nécessaire de lire les sections de ce guide dans l'ordre. Selon vos besoins, vous pouvez sauter certaines parties pour vous rendre directement à l'information qui vous intéresse. Voici quelques recommandations utiles à cet égard.

- **Vous voulez connaître les notions de base?** L'Introduction à la formation de jeunes cyberfutés (à partir de la p. 8) vous procurera un aperçu des concepts fondamentaux à cerner avant d'enseigner les pratiques cybersécuritaires, la cybersécurité et la citoyenneté numérique.
- **Vous voulez faire des liens avec le programme pédagogique de la maternelle à la 12e année?** Après l'introduction, vous trouverez le Cadre cyberfuté d'Actua (p. 21), qui décrit notre approche structurée pour former des élèves cyberfutés de la maternelle à la 12e année. Ce cadre fournit des étapes concrètes pour offrir la série d'activités MAC en classe.
- **Vous êtes déjà prête ou prêt à vous lancer?** Commencez à la section Former des jeunes cyberfutés (p. 25) afin de découvrir nos recommandations d'activités pratiques pour aider vos élèves à saisir l'importance des pratiques cybersécuritaires et de la citoyenneté numérique ainsi que leur présenter les possibilités d'emploi en cybersécurité.

Au fil de votre lecture, nous vous incitons à réfléchir aux façons dont vous pouvez adapter ce contenu pour l'intégrer à votre enseignement. Surtout, n'hésitez pas à explorer le web pour trouver d'autres ressources (crédibles et fiables!) qui vous serviront à bonifier la matière présentée ici et à créer du contenu sur mesure.

Entrons maintenant dans le vif du sujet!

Introduction à la formation de jeunes cyberfutés

Former les jeunes à l'utilisation saine, sûre et innovante des technologies, voilà l'objectif fondamental de tous les programmes de STIM d'Actua, y compris Mobilisation. Autonomisation. Connexion.

Dans le cadre de ce projet, la formation se fait sous trois angles : les pratiques cybersécuritaires, la cybersécurité et la citoyenneté numérique. Pour assurer leur sécurité en ligne, les jeunes doivent apprendre à adopter des pratiques cybersécuritaires, c'est-à-dire à faire preuve de jugement, de prudence et de proactivité à l'égard des cyberrisques. Pour utiliser l'information et les technologies de manière sûre et responsable, ils doivent connaître les outils, processus et méthodes de cybersécurité qui servent à protéger les données personnelles et les réseaux informatiques des accès non autorisés ou des cyberattaques. Enfin, pour être de bons citoyens numériques, ils doivent faire un usage responsable des contenus qu'ils consultent et partagent en ligne, respecter et inclure les autres en suivant la nétiquette, ainsi que réfléchir sérieusement avant d'agir et interagir dans le cyberespace. En formant les jeunes à ces trois aspects de la vie numérique, nous souhaitons faire en sorte qu'ils deviennent cyberfutés et puissent assurer eux-mêmes leur cybersécurité.

Dans la présente section, vous découvrirez pourquoi il est essentiel d'enseigner la cybersécurité aux jeunes, de même que les principaux concepts, enjeux et thèmes qui y sont liés. Vous verrez également comment introduire ces notions dans votre environnement d'apprentissage pour former des jeunes cyberfutés.

La sécurité en ligne pour tout le monde

Qu'est-ce qui explique l'importance accordée actuellement à la cybersécurité et aux pratiques cybersécuritaires?

1. UN NOUVEL ENJEU NATIONAL

Comme le temps passé en ligne et la complexité des cybermenaces ne cessent

d'augmenter (Centre canadien pour la cybersécurité, 2020), il est crucial que l'ensemble de la population canadienne dispose des connaissances, des compétences et des outils requis pour assurer sa sécurité et son bien-être dans le cyberespace. La sensibilisation et l'éducation du public comptent parmi les stratégies essentielles pour renforcer la sécurité nationale et individuelle. En 2018, le ministère de la Défense nationale a d'ailleurs insisté sur l'importance de l'éducation à la cybersécurité lors de l'annonce du lancement officiel de la Stratégie nationale de cybersécurité et du Centre canadien pour la cybersécurité. Ce dernier a récemment souligné qu'il s'agissait d'un enjeu national majeur en décrivant la cyberdéfense comme un sport d'équipe : « Le gouvernement, l'industrie, le milieu universitaire et les membres de la société civile doivent travailler ensemble pour renforcer la cybersécurité du Canada » (Centre canadien pour la cybersécurité, 2021).

2. PROTÉGER ET PRÉPARER LA JEUNESSE

Fréquenter le cyberespace peut s'avérer à la fois risqué et bénéfique. En plus d'être un enjeu national, l'éducation à la cybersécurité permet aux jeunes de développer des compétences numériques et des comportements sains en ligne afin d'être fin prêts pour le futur numérique. Les jeunes doivent connaître les différentes cybermenaces et les stratégies pour éviter ou contrer adéquatement celles-ci. En devenant cyberfutés, ils pourront mieux se protéger en ligne et aider leur entourage à faire de même.

Les jeunes devraient avoir des occasions de se sentir valorisés et compétents en ligne. Ils devraient aussi avoir la chance d'explorer les carrières en cybersécurité, un secteur florissant depuis quelques années. Selon le Centre canadien pour la cybersécurité, le nombre d'emplois en cybersécurité augmente de 7 % par année au Canada et 3,5 millions de postes étaient vacants à l'échelle mondiale en 2021 (Guide sur les carrières en cybersécurité, 2021). Les professionnelles et professionnels en cybersécurité sont donc très recherchés.

3. OUTILLER LA JEUNESSE

Dans le passé, on enseignait la cybersécurité et les pratiques cybersécuritaires en insistant sur les dangers du monde virtuel et le manque de compétences des utilisatrices et utilisateurs. Cette approche peut susciter de la peur, de la marginalisation et de l'impuissance chez les jeunes lorsqu'ils découvrent les risques et conséquences de l'utilisation des plateformes numériques. Ce n'est pas en les rendant craintifs que nous développerons leur citoyenneté numérique. En plus de les prévenir des cyberrisques, nous voulons aussi leur présenter les bénéfices de la présence en ligne. Nous voulons les outiller, leur fournir les compétences numériques nécessaires pour chercher de l'information en ligne et l'interpréter correctement. Les jeunes sont capables de créer des environnements virtuels inclusifs et de reconnaître et éviter les arnaques qui menacent leurs données personnelles.

Plutôt que de recourir à des histoires effrayantes, qui dépeignent les jeunes comme les cibles de cybermenaces, le présent guide explore les normes prosociales qui définissent la citoyenneté numérique responsable et les comportements appropriés en ligne. En traitant les jeunes comme s'ils étaient incapables de se protéger, on pourrait les amener à se sentir impuissants, démobilisés et déconnectés. La nécessité de proposer une autre approche, qui ne présente pas les jeunes comme des victimes, fait partie des raisons pour lesquelles nous avons créé la série « Mobilisation. Autonomisation. Connexion. » et le présent Guide pédagogique pour former des jeunes cyberfutés.

La présence en ligne

Comment décririez-vous Internet? Comment ses diverses caractéristiques influencent-elles notre vie numérique?

Internet offre de multiples moyens de communiquer. On peut y faire état de ses réflexions et de ses idées anonymement, répondre à des messages sans contraintes de temps, joindre facilement des personnes qu'on ne connaît pas dans la vraie vie, etc. Nos modes d'interaction et de socialisation ne sont pas les mêmes en ligne que hors ligne.

Par ailleurs, on constate une intégration croissante des environnements en ligne et hors ligne. Bientôt, tous les espaces constitueront peut-être des hybrides du monde réel et du monde virtuel.

Les téléphones intelligents et autres appareils connectés peuvent être transportés n'importe où. Nos maisons, écoles, véhicules, téléviseurs, appareils de conditionnement physique, feux de circulation et autres édifices et équipements sont souvent connectés à Internet, à des réseaux privés ainsi que les uns aux autres. Cela façonne inévitablement nos interactions avec nos semblables, avec les technologies et avec la planète.

Voici certaines caractéristiques clés d'Internet que vous pouvez présenter à vos élèves pour leur faire saisir l'importance d'assurer leur sécurité en ligne :

Internet est…

- **Mondial et actif en permanence.** On peut accéder instantanément, sans restriction ni interruption, à du contenu provenant du monde entier, y compris à une quantité

massive d'informations et de mésinformations. Internet est actif en permanence, c'est-à-dire qu'on peut accéder à son contenu en tout temps… mais aussi que quiconque peut accéder à nos renseignements personnels en tout temps. De plus, cette possibilité d'accéder à n'importe quoi n'importe quand a réduit notre patience et notre résilience. Aujourd'hui, on n'a plus besoin d'attendre qu'un contenu devienne disponible ni d'écouter une émission qui nous déplaît. On n'a qu'à cliquer pour choisir autre chose.

- **Interactif.** On peut interagir avec Internet et échanger avec les autres personnes présentes en ligne.
  - → **Exemples:** Publier sur les réseaux sociaux, partager des résultats de recherche ou jouer sur des plateformes de jeu virtuel.
- **Anonyme.** L'anonymat en ligne, ou la perception de celle-ci entraînent un relâchement des normes sociales parce que notre réputation n'est pas en jeu. Si cet anonymat comporte certains avantages (p. ex., en ligne, on peut échanger avec des groupes que notre cercle social habituel n'approuverait pas, ou trouver de nouvelles communautés de soutien), il peut également encourager les comportements indésirables.
  - → **Exemple:** Dans les commentaires publiés sous les vidéos, les billets de blogues, etc., certains internautes tiennent un langage injurieux ou des propos intimidants qu'ils n'utiliseraient jamais devant ou une interlocutrice un interlocuteur en chair et en os.
- **Addictif.** Certaines caractéristiques d'Internet sont conçues pour nous garder en ligne et nous faire dépenser de l'argent afin de jouer à des jeux, de visionner du contenu ou de partager de l'information. La nature ludique et addictive d'Internet n'est pas accidentelle et nombreux sont ceux qui tirent profit de notre utilisation des appareils connectés. Lorsqu'on garde en tête qu'une bonne partie du contenu en ligne a pour but d'obtenir de l'information à notre sujet et de nous vendre des produits ou des idées, on peut poser un regard critique sur le temps qu'on passe sur le web et notre utilisation des technologies. On commence seulement à examiner les effets des médias sociaux sur les gens, et sur les jeunes en particulier.
- **Collaboratif.** On peut publier une grande quantité d'information sous de multiples formes et dans divers médias sociaux. Et chaque fois que cette information est partagée (republiée telle quelle ou remodelée), sa portée s'amplifie.
  - → L'inconvénient du partage, c'est que cela peut fausser notre perception de ce qui constitue une information digne d'attention. L'avantage, c'est que l'information importante peut être diffusée rapidement à large échelle. Quoi qu'il en soit, pour assurer notre sécurité en ligne, il est fondamental de jeter un regard critique sur notre consommation de contenus sur les médias sociaux (vidéos, articles, images, etc.).
- **Une chambre d'échos.** Sur Internet, il existe une multitude d'espaces virtuels, comme des babillards électroniques et des sites de socialisation, où l'on peut trouver des croyances et des opinions qui rejoignent directement les nôtres et les renforcent.

- Si on fréquente le web sans être conscientes ou conscients de ces chambres d'échos, on ne sera peut-être jamais exposés à des idées et opinions différentes des nôtres, ou même à de l'information basée sur des données probantes. Internet est un endroit merveilleux pour trouver des communautés de pensée, mais il peut aussi être un lieu effrayant, où les forces puissantes de la pensée unique manipulent facilement nos opinions. Les algorithmes jouent un rôle important à cet égard, car ils suivent nos activités à la trace afin de cerner nos préférences et de nous proposer d'autres contenus similaires. S'ils sont utiles pour trouver rapidement l'information ou les communautés qu'on recherche, ils peuvent aussi être très limitants et parfois même dangereux.
    - **Exemples:** Les médias sociaux comme TikTok qui vous « montrent » des vidéos que vous pourriez trouver drôles ou qui « conviennent parfaitement » à vos goûts; les publicités ciblées; les invitations à vous joindre à des groupes semblables à ceux dont vous faites partie; etc.o
    - **Mise en garde :** Les algorithmes ne sont pas conçus pour servir vos intérêts, mais bien les objectifs des développeurs, qui veulent vous montrer plus de publicités ou tenter d'influencer votre opinion.

Survol des principaux thèmes à aborder pour former des jeunes cyberfutés

Quels sont les différents sujets associés à la cybersécurité et aux pratiques cybersécuritaires?

1. CITOYENNETÉ NUMÉRIQUE

La citoyenneté numérique renvoie à la capacité d'une personne à comprendre et à utiliser adéquatement Internet. En tant que citoyennes et citoyens numériques, nous travaillons, apprenons et socialisons dans des espaces virtuels connectés. Pour fréquenter ces cyberespaces en toute sécurité, nous devons savoir comment protéger nos renseignements personnels, comment communiquer avec les autres de manière positive et inclusive, et comment jeter un regard critique sur l'information que nous trouvons en ligne.
Nous devons aussi connaître et apprendre à éviter ou contrer les nombreuses menaces auxquelles nous sommes exposés, comme les violations de données, la cyberintimidation, l'hameçonnage, la mésinformation, les comportements et contenus inappropriés et le vol d'identité.

Les bonnes citoyennes et bons citoyens numériques font preuve de jugement critique, de leadership, de bienveillance et de responsabilité.

Pour ce faire, elles et ils doivent bien comprendre ce que sont la **cybersécurité, la nétiquette et le bien-être numérique**. Les bonnes citoyennes et bons citoyens numériques font preuve de jugement critique, de leadership, de bienveillance et de responsabilité.

2. IDENTITÉ VIRTUELLE ET EMPREINTE NUMÉRIQUE

Lorsqu'on utilise des appareils connectés, on développe une identité virtuelle. Nos publications sur les médias sociaux, nos interventions sur les plateformes de jeu et nos autres interactions en ligne font partie de nos moyens d'expression dans le cyberespace. L'identité virtuelle diffère de l'identité « réelle » de nombreuses façons. Lorsqu'on est jeune et q u'on explore encore son identité et ses valeurs, il peut être tentant d'adopter des personas en ligne, mais cela ne se fait pas sans danger. Il ne faut pas oublier que la plupart sinon l'ensemble de nos actions en ligne laissent des traces numériques permanentes. Notre identité numérique se compose aussi de données auxquelles on n'a pas accès. Par exemple, Fitbit recueille des données sur la fréquence de vos séances d'exercices et Netflix, sur les types de contenu que vous visionnez. Elles peuvent ensuite relier ces données au profil qu'elles ont dressé à votre sujet. Tous les dispositifs connectés et toutes les plateformes web contribuent à dessiner votre empreinte numérique.

3. SÉCURITÉ DES DONNÉES ET CONFIDENTIALITÉ

Plus nombreux sont les sites web et outils qui recueillent nos renseignements personnels, plus le risque de violation de ces renseignements augmente. Pour bien protéger nos données, il faut évaluer les risques de chaque situation en adoptant un point de vue critique et un comportement cybersécuritaire. Avant de divulguer des renseignements sur un site web, une plateforme de jeu ou une boutique en ligne, il faut veiller à bien comprendre la politique sur la protection des renseignements personnels. Plutôt qu'accepter rapidement les conditions d'utilisation, il est conseillé de prendre le temps de les lire et de bien réfléchir à ce que cela implique (*voir Connaissances des lois, libertés et responsabilités en matière de cybersécurité à la p. 19 pour en savoir plus*).

Par exemple, on peut vous demander votre date d'anniversaire sur une plateforme de musique en continu, dans un formulaire d'inscription ou sur un site de jeux gratuits. Cependant, chacun de ceux-ci a fort probablement des pratiques et des politiques différentes à l'égard de la protection, de l'enregistrement et de la transmission des renseignements personnels. Pensez-y : la diffusion de vos données personnelles constitue souvent le paiement exigé pour obtenir un produit ou service; est-ce que cela en vaut toujours la peine?

4. SANTÉ MENTALE ET BIEN-ÊTRE NUMÉRIQUE

La santé mentale et le bien-être comptent autant en ligne que hors ligne. C'est pourquoi il faut être consciente ou conscient de ce qu'on consomme en ligne et du temps qu'on y passe.

Prenez régulièrement le temps de réfléchir à la façon dont vous vous sentez après avoir vu ou lu un contenu sur le web ou après une longue séance de navigation. Cela vous aidera à évaluer votre niveau de bien-être dans le cyberespace et votre relation avec Internet.

En tant qu'enseignante ou enseignant, montrez à vos élèves à prendre ces moments de recul et de réflexion. Vous les aiderez à développer des stratégies utiles pour fréquenter sainement Internet.

5. CYBERARNAQUES ET CYBERCRIMES

Les arnaques et les crimes commis en ligne varient en complexité et en gravité. Les cybercrimes comme le piratage informatique, le vol d'identité et l'exploitation des enfants constituent des actes punissables par la loi. D'autres cybercrimes, comme les tentatives d'**hameçonnage**, sont plus banals et font pratiquement partie de notre quotidien. Nombre de tentatives de vol de données personnelles, financières ou intellectuelles sont évidentes, par exemple une fenêtre intruse clignotante qui affiche « Croisière gratuite ». D'autres escroqueries peuvent nous prendre par surprise, comme un message qui apparaît sur un site fiable et nous invite à « Remplir ce sondage pour gagner un iPhone ». Certaines arnaques sont très convaincantes et impossibles à distinguer d'une communication légitime, par exemple un courriel provenant d'un expéditeur connu vous prévenant que votre mot de passe a été « compromis » et doit être mis à jour.

Meilleures pratiques cybersécuritaires

1. Passez en revue et réglez vos paramètres de sécurité.
2. Ne fournissez que les renseignements personnels absolument requis pour utiliser une application ou un service.
3. Faites confiance, mais vérifiez. Les apparences sont parfois trompeuses sur Internet.
4. Connectez-vous uniquement à des réseaux Wi-Fi sécurisés (autrement, évitez d'accéder à vos comptes et utilisez uniquement un RPV fiable).
5. Pour éviter de télécharger des logiciels malveillants, réfléchissez avant de cliquer sur un lien, de télécharger un fichier ou d'accepter quoi que ce soit.
6. Créez des mots de passe forts et gérez adéquatement votre liste de mots de passe.
7. Considérez tout ce que vous faites en ligne comme du contenu permanent et potentiellement public, qui contribue à votre empreinte numérique.
8. Mettez à jour tous vos logiciels et dotez-vous d'un antivirus.
9. Sur vos pages personnelles (Instagram, Snapchat), n'échangez qu'avec des personnes que vous connaissez dans la vraie vie; sinon, évitez de communiquer vos renseignements personnels (nom, adresse, date de naissance, etc.).

Les risques du cyberespace pour les jeunes

Les jeunes doivent être au courant des risques et bénéfices de la technologie.

Ils font face aux mêmes risques, arnaques et crimes que les adultes, en plus d'être exposés à l'exploitation, au sextage et à la cyberintimidation. Personne ne veut se sentir inconfortable, inquiet ou exploité. La création d'un espace sûr, où l'on peut discuter sans crainte de ses sentiments, peut donc constituer une bonne stratégie pour lancer la conversation à propos des risques du cyberespace.

Quels dangers menacent les jeunes en ligne et comment peut-on leur enseigner à se protéger?

ENJEUX DE SÉCURITÉ ET DE CONFIDENTIALITÉ

Les jeunes partagent couramment leurs mots de passe et leurs codes de déverrouillage avec leurs amies et amis sans saisir les risques que cela comporte. S'ils perçoivent souvent cette pratique comme une marque de confiance, elle pose néanmoins des enjeux de sécurité et de confidentialité, car elle permet à d'autres personnes qu'eux d'accéder à leur compte et à leur profil (Kaspersky, 2018).

De plus, si les jeunes utilisent les mêmes mots de passe et noms d'utilisateur pour plusieurs comptes, des fraudeurs pourraient accéder à ceux-ci en utilisant le bourrage d'identifiants.

En outre, comme de nombreux jeunes consultent Internet à partir de la tablette ou de l'ordinateur familiaux, ils ont potentiellement accès aux renseignements de carte de crédit et aux mots de passe qui y sont enregistrés, et donc aussi les personnes qui tentent d'obtenir cette information. En revanche, le partage d'appareils peut s'avérer bénéfique pour toute la famille lorsqu'un de ses membres devient cyberfuté!

VOTRE RÔLE COMME ENSEIGNANTE OU ENSEIGNANT.

Il peut être tentant de communiquer à nos amies ou amis nos mots de passe de réseaux sociaux ou de jeux, ou encore les données de connexion de notre compte à la bibliothèque, mais ce n'est JAMAIS une bonne idée. Rappelez cela à vos élèves lorsqu'ils accèdent à leur compte étudiant sur un ordinateur partagé ou même sur leur propre appareil.

VOLS D'IDENTITÉ CIBLANT LES ENFANTS

Il peut paraître étonnant que des pirates informatiques veuillent voler l'identité d'un enfant; pourtant, ce type de cybercrime est en hausse. Si un enfant fournit suffisamment de renseignements personnels en ligne, un cybercriminel peut s'emparer de son identité pour perpétrer des crimes sous son nom ou pour commettre des fraudes financières qui ne seront détectées que beaucoup plus tard, lorsque le jeune fera une demande de crédit. Pour se prémunir contre ces types de crimes, les jeunes doivent agir avec précaution et bien réfléchir avant de transmettre des renseignements personnels comme leur nom complet, leur date de naissance et leur adresse.

VOTRE RÔLE COMME ENSEIGNANTE OU ENSEIGNANT.

Évitez d'utiliser des sites exigeant que vos élèves fournissent des renseignements personnels pour se créer un compte. De plus, rappelez-leur ceci : lorsqu'ils accèdent à un site pour la première fois, de la maison ou de l'école, ils devraient se demander pourquoi on leur demande de fournir de l'information, éviter de divulguer des renseignements personnels et utiliser un alias ou un surnom plutôt que leur vrai nom au complet. Sauf sur un site officiel, ils peuvent falsifier leur date d'anniversaire, par exemple pour s'inscrire sur une plateforme de jeu.

LE SURPARTAGE

La tension entre la protection de la vie privée et le partage de ses expériences avec la communauté est inhérente aux réseaux sociaux. Compte tenu de l'omniprésence des réseaux sociaux dans leur vie, les jeunes tendent à privilégier les liens avec la communauté plutôt que la confidentialité.

> **Certains diront « Je n'ai rien à cacher » ou « Je ne fais rien de mal ou d'illégal en ligne, alors pourquoi devrais-je me soucier de mon empreinte numérique? ».**

Or, la confidentialité n'a rien à avoir avec la dissimulation. Elle concerne le contrôle des données qui nous appartiennent et ce que les autres peuvent en faire.

VOTRE RÔLE COMME ENSEIGNANTE OU ENSEIGNANT.

Responsabilisez les jeunes. Expliquez-leur qu'ils peuvent contrôler leur consommation d'information et la création de leur identité en ligne en réfléchissant sérieusement à ce qu'ils font sur les réseaux sociaux et en tirant le maximum des paramètres de confidentialité. Expliquez-leur ce que sont le surpartage et les renseignements personnels afin de les aider à bien saisir le concept de confidentialité et les conséquences d'une violation de données. Posez-leur ces questions : Quelle information devrait rester confidentielle? Qui doit avoir accès à cette information? Savez-vous avec qui vous partagez cette information?

CYBERINTIMIDATION, HARCÈLEMENT ET EXPLOITATION

La cyberintimidation demeure un problème grave et généralisé chez les jeunes. Cela ne se résume pas à publier des commentaires blessants; cela consiste entre autres à répandre des rumeurs par texto, à créer un faux compte sur un réseau social, à usurper l'identité d'une autre personne pour nuire à sa réputation, à transférer une photo embarrassante de quelqu'un, à partager des photos intimes qui ne nous appartiennent pas ou encore à troller ou traquer quelqu'un en ligne. On minimise souvent la cyberintimidation, alors qu'elle peut inclure la distribution de pornographie infantile (p. ex. la transmission de photos personnelles compromettantes ou intimes d'une personne de moins de 18 ans, même si les destinataires sont d'autres mineurs), l'extorsion, le harcèlement, la diffamation et la violence conjugale.

La cyberintimidation est souvent subtile, mais persistante. Vu de l'extérieur, ce type de comportement en ligne peut paraître banal puisque les jeunes se font souvent des blagues ou des commentaires méprisants ou dénigrants. Pourtant, la cyberintimidation, le harcèlement et l'exploitation peuvent entraîner de l'isolement, une faible estime de soi et des problèmes de santé mentale comme la dépression, des troubles alimentaires et de l'automutilation.

VOTRE RÔLE COMME ENSEIGNANTE OU ENSEIGNANT.

Introduisez le sujet de la cyberintimidation dans vos conversations sur l'intimidation en général. Parlez avec vos élèves des incidents dont ils sont témoins et de la façon dont ils gèrent cela. Plusieurs des stratégies servant à contrer l'intimidation dans la vie réelle sont applicables à la cyberintimidation. Les incidents de cyberintimidation ou de harcèlement peuvent survenir après les heures de classe (avec des pairs ou des étrangers) et les élèves doivent savoir comment les reconnaître. Ils doivent également connaître les mesures à prendre pour se protéger et protéger les autres, de même que comprendre comment leur propre comportement peut être perçu comme de la cyberintimidation. Aidez-les à trouver des lieux sûrs où signaler des incidents de cyberintimidation, y compris directement sur les réseaux sociaux qu'ils utilisent.

Offrez aux jeunes des occasions de parler de leurs interactions virtuelles et encouragez-les à réfléchir régulièrement à leur bien-être en ligne. Comme ils peuvent être à la fois des cyberintimidateurs et des victimes, ils devaient se poser les questions suivantes : Est-ce que je me sens bien après avoir parlé à cette personne? Est-ce que je suis à l'aise avec les questions posées par cette personne? Est-ce que je suis fier de la façon dont j'ai traité cette personne? Est-ce que je voudrais que tout le monde sache que c'est moi qui ai publié ce commentaire?

LA PSYCHOLOGIE SOCIALE ET INTERNET

Si nos interactions avec les autres en ligne peuvent susciter beaucoup d'émotions, il en va de même pour nos interactions avec le contenu et l'information qu'on consulte, visionne ou publie. Le bouton « J'aime » est un exemple parfait de la façon dont les émotions et la psychologie sociale sont liées au temps passé en ligne.

> **Il y a une réaction chimique dans notre cerveau lorsqu'on obtient des réactions positives comme des « J'aime » sur les réseaux sociaux.**

Inversement, on peut éprouver de la déception lorsque notre contenu n'est pas approuvé. Les jeunes ont à leur portée un vaste éventail de contenus susceptibles d'influencer la façon dont ils veulent paraître ou agir. Par exemple, s'ils suivent de nombreuses vedettes et ont de la difficulté à distinguer le monde virtuel de la réalité, ils peuvent avoir des attentes irréalistes à l'endroit d'eux-mêmes (p. ex. sur les plans de l'image corporelle, des relations ou de la richesse).

VOTRE RÔLE COMME ENSEIGNANTE OU ENSEIGNANT.

Donnez aux jeunes du pouvoir sur leur relation avec Internet et les technologies. Dites-leur que ce sont eux qui utilisent ces outils, et non l'inverse. Montrez-leur qu'ils peuvent et doivent contrôler leurs activités, leur présence et leur empreinte en ligne. Insistez sur les conséquences à long terme de leurs actions dans le cyberespace, sur les traces permanentes qu'ils laissent en ligne et sur la façon dont celles-ci forgent la perception qu'on a d'eux.

Connaissances des lois, libertés et responsabilités en matière de cybersécurité

Qu'est-ce que les jeunes devraient savoir sur les lois, droits, libertés et responsabilités en matière de cybersécurité?

Il existe plusieurs lois sur la protection de la vie privée au Canada. Certaines visent les établissements publics comme les écoles, d'autres la consommation et d'autres encore les données personnelles sur la santé. Ces lois sont encadrées par le commissaire à la protection de la vie privée du Canada et des commissaires provinciaux. Elles devraient être mises à jour dans les prochaines années afin de mieux refléter l'évolution des technologies et ses conséquences. Au Canada, les citoyennes et citoyens ont le droit de demander une copie de leurs données. Par exemple, vous pouvez demander à une entreprise de vous transmettre tous les renseignements qu'elle a enregistrés à votre sujet. Ainsi, en 2020, un homme a demandé à Tim Hortons de lui transmettre toutes les données recueillies à son sujet à l'aide de son application mobile.

Il a été choqué de constater que l'entreprise le localisait en tout temps, et pas seulement lorsqu'il passait une commande. Comme cela allait à l'encontre de la politique sur la protection de la vie privée de Tim Hortons, l'homme a pu porter plainte auprès du Commissariat à la protection de la vie privée.

La plupart des applications et des services que nous utilisons proviennent des États-Unis (p. ex. Google et Facebook).

Bien que nous ayons certains droits en tant que cityonnes et citoyens canadiens, nous demeurons soumis aux lois qui permettent au gouvernement américain d'accéder à nos données conservées aux États-Unis. Si vous vivez en Europe, vos données sont protégées par le Règlement général sur la protection des données (RGPD) de l'Union européenne. Cette législation est l'une des plus strictes au monde. Elle accorde la priorité à l'individu et l'autorise même à demander que ses données soient supprimées d'un système. Nous espérons que le Canada se dotera éventuellement d'un tel règlement.

QU'EN EST-IL DES DONNÉES PERSONNELLES DES JEUNES?

Il faut noter que, dans la plupart des cas, il est interdit de recueillir les renseignements personnels d'un enfant de moins de 13 ans, à moins qu'il s'agisse d'une application ou d'un service conçus spécifiquement pour les jeunes. Par exemple, la loi autorise uniquement les personnes de 13 ans et plus à utiliser Instagram (en raison de la publicité et de la revente des données personnelles), alors que les jeunes de tous âges peuvent accéder sans restriction à Google Workspace for Education, car ce service est conçu pour les enfants (pas de collecte ni de revente de données personnelles). Il est important que le personnel enseignant, les parents et les jeunes choisissent des applications et des services destinés à la jeunesse. Autrement, les jeunes pourraient transmettre plus de données à leur sujet qu'ils en ont conscience. Quant aux plus de 13 ans, ils doivent comprendre les risques d'accepter la politique de confidentialité et les conditions d'utilisation d'un produit ou d'un service. La plupart des jeunes et de nombreux adultes ne lisent pas ces documents. La politique de confidentialité explique quelles données sont recueillies par l'application ou le service, dans quels buts et avec qui elles sont partagées.

Les conditions d'utilisation indiquent le fonctionnement du produit ou du service et la façon dont on s'attend à ce que vous l'utilisiez. Si certains usages sont interdits, ceux-ci seront énoncés dans les conditions d'utilisation, de même que les conséquences du non-respect de ces conditions.

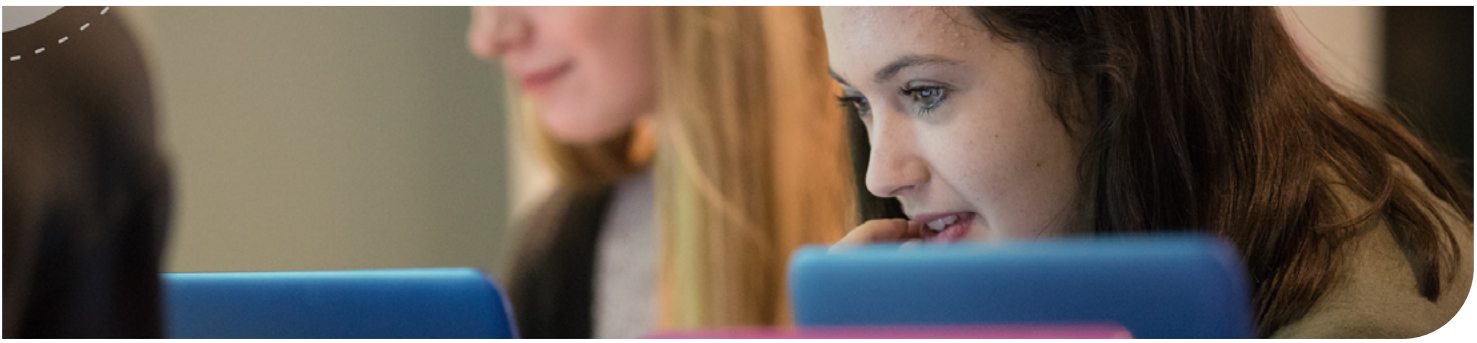
Tous les internautes doivent bien comprendre qu'on leur demande de partager leurs renseignements personnels en échange de l'utilisation d'un produit. Rien n'est gratuit. Si vous ne payez pas pour un produit, c'est que vous êtes le produit.

Cadre cyberfuté du projet MAC d'Actua

Le Cadre cyberfuté d'Actua a été créé au début de 2021, en collaboration avec des spécialistes de la cybersécurité, des responsables des services policiers, des enseignantes et des enseignants et d'autres expertes et experts du domaine.

Ce cadre sert à orienter les approches et les contenus développés pour le projet MAC d'Actua, tout en fournissant au personnel enseignant un aperçu des concepts clés et des objectifs d'apprentissage destinés à former des jeunes cyberfutés.

Vous trouverez les versions anglaise et française de ce cadre ci-dessous ainsi qu'en format téléchargeable sur actua.ca.



Les prémisses du cadre

Les jeunes sont curieux, ils cherchent à créer des liens, ils explorent et définissent leur identité et leurs champs d'intérêt. Leurs relations sont primordiales et ils accordent beaucoup d'importance aux amies, amis et à la famille lors de la prise de décisions. Ces caractéristiques distinctives de l'adolescence ne sont pas fondamentalement négatives (en fait, elles sont très précieuses!), mais elles peuvent présenter un risque pour les jeunes qui ne connaissent pas les pratiques cybersécuritaires.

Les jeunes sont soumis à des facteurs de risque spécifiques, qui les rendent particulièrement vulnérables aux pressions sociales, à la victimisation en ligne et à la cyberinsécurité. Les jeunes adultes sont en processus de développement de leur identité individuelle et sociale, et cette

recherche de sens ou d'appartenance peut les exposer à des comportements dangereux ou nuisibles en ligne, que ce soit les leurs ou ceux des autres; par exemple, le piratage informatique, la pression des pairs, l'hameçonnage et les fausses informations. Le Cadre cyberfuté d'Actua a été élaboré dans le but d'aider les jeunes à devenir des citoyens numériques responsables, aptes à reconnaître les différents cyberrisques et à appliquer des stratégies pour fréquenter le web de manière futée et sécuritaire.

Composantes du cadre

Idées générales

Le cadre repose sur trois piliers – Mobilisation, Autonomisation et Connexion –, et chacun de ceux-ci est associé à une idée générale. Le pilier **Mobilisation** prépare les jeunes à assurer leur sécurité en ligne en les dotant d'outils essentiels et de solides connaissances de base sur la cybersécurité et les pratiques cybersécuritaires. Le pilier **Autonomisation** leur permet de mettre en pratique leurs connaissances dans une variété de situations et de contextes. Et le dernier pilier, **Connexion**, met l'accent sur le développement de relations saines en ligne et hors ligne.

Thèmes

Chaque idée générale se divise en plusieurs thèmes. Il s'agit de sujets concrets et suffisamment généraux pour convenir à divers groupes d'âge et niveaux de compétences, de novice à expert, selon la quantité de détails techniques fournis

Par exemple, pour le thème « données et documentation en ligne » (du pilier Mobilisation), on pourrait parler des noms d'utilisateurs et des mots de passe au primaire; puis, au secondaire, expliquer ce que sont les mégadonnées, la façon dont les jeux de données nourrissent les algorithmes et la manière dont nos renseignements personnels peuvent orienter les décisions d'une entreprise concernant ses produits.

Objectifs d'apprentissage

De la même manière que les idées générales mènent à plusieurs thèmes, chacun de ces thèmes vise des objectifs d'apprentissage spécifiques, qui sont essentiels pour la formation de jeunes cyberfutés. Nous souhaitons qu'à la fin du secondaire, toutes et tous les élèves aient atteint l'ensemble des objectifs et disposent d'une formation de base sur la cybersécurité, les pratiques cybersécuritaires et la citoyenneté numérique. Ces objectifs représentent les connaissances et compétences fondamentales dont une personne a besoin pour assurer sa sécurité en ligne, peu importe son niveau d'habiletés techniques. En fait, nous les avons formulés afin de répondre aux besoins des élèves qui n'étudient pas les technologies et l'informatique. Autrement dit, pour comprendre les concepts abordés, aucune expertise en programmation ou en informatique n'est requise.

actüa
Jeunesse · STIM · Innovation

Cadre Cyber Futé d'Actua

	Mobilisation	Autonomisation	Connexion
Idées générales	Il est essentiel d'équiper les jeunes d'outils (connaissances) de sensibilisation à la cybersécurité afin de les inciter à faire un usage responsable de la technologie.	La possibilité de mettre ses compétences en pratique et de traduire ses connaissances en action ou en création permet de former une génération de jeunes cyberavertis.	L'acquisition d'une attitude cyberavertie repose sur la fréquentation de communautés bienveillantes et le maintien de saines relations en ligne et hors ligne. Elle contribue à l'exemplarité en matière d'apprentissage continu, de pensée critique et de recherche des moyens voulus pour assurer durablement la cybersécurité.
Thèmes	• Cybersécurité • Identité numérique (par ex. bourrage d'identifiants) • Données et documentation en ligne • Protection de la vie privée, réseaux privés virtuels (VPN)	• Liens entre les données et l'intelligence artificielle (IA) • Crédibilité, biais et mésinformation • Intention des interactions en ligne, protection et réduction des méfaits • Collecte d'information par logiciel en libre essai	• Expression de soi • Comportement social et relations saines • Interactivité/plateformes orientées réseau • Renforcement des communautés, connectivité globale
Objectifs d'apprentissage **(Les élèves auront l'occasion de...)**	• Acquérir des notions de littératie numérique; faire preuve d'usage responsable de la technologie. • Expliquer les avantages de la technologie sur les plans intellectuel, pratique et créatif. • Déterminer les risques associés à la navigation sur Internet ou aux réseaux connectés (par ex. Internet des objets) et prendre les mesures voulues pour les prévenir. • Acquérir une connaissance fondamentale des environnements numériques de façon à devenir des usagers avertis, plutôt que d'être manipulés par les outils et ignorants des technologies et des données qu'ils utilisent.	• S'initier à des pratiques cybersécuritaires (par. ex. créer des mots de passe robustes, s'abstenir de divulguer ou de violer la confidentialité des renseignements personnels). • Apprendre à distinguer les sources partiales des sources fiables en matière d'information. • Apprendre à interpréter les intentions des individus et des groupes présents sur le web.	• Développer un sentiment d'identité positif en ligne et hors ligne. • Apprendre à reconnaître les interactions appropriées et à prévenir la cyberintimidation et les méfaits. À se servir de la technologie pour bâtir des réseaux sociaux bienveillants. • Apprendre à observer un comportement prudent dans le cyberespace : protection des renseignements personnels, interactions positives et relations appropriées avec les inconnus. • Connaître leurs droits et savoir où se tourner pour obtenir de l'aide en cas d'atteinte à leur sécurité.
Liens avec les programmes pédagogiques Synthétisé à partir du Cadre de référence pancanadien pour l'enseignement de l'informatique	**CYBERSÉCURITÉ** : Définir la cybersécurité; créer des mots de passe sûrs en utilisant des critères efficaces; Décrire les cyberattaques courantes et les contenus malveillants et évaluer; Appliquer des pratiques de prévention. **DONNÉES – GOUVERNANCE DES DONNÉES**: Comprendre comment les données numériques sont créées grâce à l'activité numérique et physique et réfléchir à qui possède les données qu'ils produisent; Réfléchir et utiliser les paramètres de confidentialité sur les plateformes en ligne. **TECHNOLOGIE ET SOCIÉTÉ – ÉTHIQUE, SÉCURITÉ ET DROIT** : Identifier des stratégies pour protéger leurs données personnelles et leur identité en ligne; Expliquer les problèmes de confidentialité; Évaluer les effets de la criminalité numérique sur soi-même et la société.		

Liens avec le programme cadre : la formation d'élèves cyberfutés de la maternelle à la 12e année

Le but général du **Cadre cyberfuté du projet MAC** est de fournir aux élèves une formation en cybersécurité suffisante pour qu'ils puissent participer à des conversations sur le sujet, adopter un point de vue critique en ligne et connaître les possibilités de carrière dans ce domaine. Ce cadre s'aligne directement avec trois aspects clés du Cadre de référence pancanadien pour l'enseignement de l'informatique :

1. **Cybersécurité**
   - Compétences et pratiques : Définir la cybersécurité; créer des mots de passe sûrs en utilisant des critères efficaces; décrire et évaluer les cyberattaques courantes et les contenus malveillants; appliquer des pratiques de prévention.
2. **Données (Gouvernance des données)**
   - Compétences et pratiques : Comprendre comment les données numériques sont créées grâce aux activités numériques et physiques; réfléchir à la propriété des données qu'on produit; utiliser les paramètres de confidentialité des plateformes en ligne.
3. **Technologie et société (Éthique, sécurité et droit)**
   - Compétences et pratiques : Décrire des stratégies pour protéger ses données personnelles et son identité en ligne; expliquer les problèmes de confidentialité; évaluer les effets de la cybercriminalité sur soi-même et la société.

En intégrant notre Cadre cyberfuté au Cadre de référence pancanadien pour l'enseignement de l'informatique, nous proposons une feuille de route pour introduire les pratiques cybersécuritaires, la cybersécurité et la citoyenneté numérique dans les cours d'informatique, de même que dans l'enseignement de matières non techniques.

Former des jeunes cyberfutés

En même temps que son Cadre cyberfuté, Actua a mis au point une série d'activités pratiques et interactives qui permettent au personnel enseignant de réinventer l'éducation à la cybersécurité.

Conseils pour mobiliser les jeunes

1. CHOISISSEZ LES BONS MOTS !

- **Mettez l'accent sur les capacités de vos élèves plutôt que sur leur manque de compétences** : Il est crucial d'adopter un langage positif et valorisant afin que les jeunes ne craignent pas de fréquenter le cyberespace. Oui, nous voulons les prévenir des risques, mais en leur transmettant des compétences clés qui les aideront à développer l'assurance requise pour naviguer sur le web de manière sûre et futée.
  - « Internet peut être une excellente ressource » plutôt que « Internet est un endroit effrayant »
  - « Il faut se poser les bonnes questions » plutôt que « Il faut toujours être sur ses gardes et prête ou prêt à se protéger »
- Utilisez des normes prosociales : Les recherches démontrent que, pour illustrer l'importance d'assurer sa sécurité sur Internet, il vaut mieux donner des exemples de bonnes décisions en ligne plutôt que d'attirer l'attention sur des incidents controversés ou des conséquences néfastes.

2. COMMENCEZ DÈS QUE POSSIBLE

- Il n'y a pas de meilleur moment que maintenant. Il est essentiel d'aborder ce sujet dès que possible, mais veillez à l'adapter au groupe d'âge de vos élèves. Pour ce faire, vous devez d'abord vous familiariser avec la matière, et la consultation du présent guide constitue un bon point de départ.

3. CRÉEZ UN ESPACE DE DIALOGUE SÛR ET ACCUEILLANT

- Si vos élèves se sentent à l'aise de parler de ce qu'ils vivent en général (pas seulement sur Internet), ils auront moins d'hésitation à discuter des problèmes qu'ils rencontrent en ligne.
  - Gardez le canal de communication ouvert (ça ne devrait pas être la première ni la dernière fois qu'ils expriment leurs pensées!)
  - Parlez aussi de vos expériences (pour faciliter l'identification)

4. USEZ DE CRÉATIVITÉ ET TROUVEZ DES FAÇONS D'INTÉGRER LE SUJET DANS VOTRE PROGRAMME

- Comme mentionné ci-dessus, commencez par vous familiariser avec la cybersécurité afin de pouvoir établir des liens avec les autres matières enseignées.
- Suggestions :
  - Abordez le sujet chaque fois que vos élèves font une activité sur Internet (p. ex. les partis pris médiatiques et les fausses idées)
  - Commencez chaque cours par une petite activité, puis faites-y référence dans vos discussions de groupe à divers moments de la journée.
  - Intégrez le sujet des pratiques cybersécuritaires dans divers volets de votre programme afin de créer de multiples occasions de renforcer les comportements sains en ligne et de parler des comportements problématiques.
  - Des activités d'approfondissement sont fournies dans chacun des six modules pour vous permettre d'adapter le contenu aux besoins des élèves plus âgés.

5. PARLEZ DE CITOYENNETÉ NUMÉRIQUE EN PLUS DE CYBERVICTIMISATION

- L'enseignement des pratiques cybersécuritaires et de la cybersécurité ne portent pas uniquement sur les dangers du cyberespace.
- Nous voulons inciter les élèves à devenir des citoyennes et citoyens numériques avertis et responsables en leur montrant comment utiliser les technologies numériques de manière efficace et appropriée.

6. FAVORISEZ LA PARTICIPATION ET LA COLLABORATION DES ÉLÈVES

- Les tendances et les technologies évoluent constamment, et les jeunes sont souvent

plus au fait de celles-ci que nous.

- Pour rester à l'affût de l'actualité numérique, créez un espace où les jeunes peuvent partager leurs connaissances et leurs points de vue sur le sujet et collaborer pour résoudre des problèmes. Encouragez les discussions entre élèves, prenez des notes et adaptez votre contenu en conséquence.

7. DÉVELOPPEZ LA CAPACITÉ D'EMPATHIE DE VOS ÉLÈVES

- Au fur et à mesure qu'ils évoluent dans le monde, les jeunes peuvent éprouver des problèmes personnels (crise d'identité, ruptures amicales ou amoureuses, difficultés scolaires, sentiments d'injustice, problèmes d'intégration, isolement, problèmes d'image corporelle, troubles alimentaires, dysphorie, etc.). Il est important de garder cela à l'esprit lorsqu'on leur enseigne à naviguer dans le cyberespace en toute sécurité ainsi qu'à entretenir des relations saines avec les autres et eux-mêmes.
- L'empathie compte autant en ligne que hors ligne, et il s'agit d'un outil clé pour traiter des activités nuisibles en ligne.
- Il n'est pas toujours facile de faire preuve d'empathie en ligne pour diverses raisons (peu de conséquences apparentes, anonymat, réactions mal interprétées, désinhibition, etc.), mais c'est tout de même important. On fait souvent une distinction entre les activités en ligne et hors ligne. Or, cette séparation n'est qu'un mythe qu'il faut abattre. Les jeunes doivent comprendre que leurs actions virtuelles ont vraiment un impact dans la vie réelle.

8. FOURNISSEZ DES DÉFINITIONS CLAIRES ET CONCRÈTES

- Les jeunes ont probablement déjà une compréhension erronée de certains termes. Veillez à fournir des exemples concrets, clairs et diversifiés pour les termes présentés.
- Selon Bazelon (2013), il faut éviter les étiquettes. Par exemple, peu de jeunes acceptent d'être qualifiés de « victime » ou d'« intimidateur ». Plutôt que de parler ouvertement de leurs comportements (même s'ils correspondent à la définition), ils vont refuser de les reconnaître afin d'éviter la stigmatisation et l'impact émotionnel.

9. TENEZ COMPTE DU FAIT QUE CERTAINS JEUNES N'ONT PAS D'APPAREIL

- Il est important de reconnaître que l'accès aux technologies et à Internet varie. Si certains jeunes peuvent accéder à Internet à partir de leur propre appareil, d'autres ne peuvent le faire que sur la tablette ou l'ordinateur familiaux, ou uniquement à l'école.

→ Tenez compte de cela lorsque vous animez des discussions. Cela vous aidera à mieux connaître les diverses expériences de vos élèves en ligne.

10. ACCORDEZ DE L'IMPORTANCE À LA PERTINENCE ET À LA REPRÉSENTATION

→ Passez en revue votre contenu et trouvez des façons de le rendre encore plus pertinent pour vos élèves. Faites en sorte qu'elles et ils puissent s'y reconnaître et faire des liens avec leur propre réalité.

→ Examples:

- Proposez aux élèves des articles traitant de sujets pertinents pour leur communauté (activité : détective numérique)
- Encouragez tous les élèves à se représenter dans les images qu'elles et ils créent à la fin de chaque activité (affiches, infographies, etc.)
- Invitez des personnes des genres variés et de diverses origines à venir parler de cybersécurité en classe

Glossaire

Terme	Définition
Accès numérique	Capacité à utiliser pleinement Internet et les technologies. Cette capacité peut être entravée par l'absence de connexion Internet, le manque de mesures d'accessibilité pour les personnes handicapées, etc.
Authentification multifacteur	Processus de sécurité qui recourt à un autre mode d'authentification de l'utilisateur en plus du mot de passe. Il peut s'agir d'une demande de confirmation envoyée à une adresse de courriel secondaire ou par texto.
Base de données	Ensemble d'éléments d'information structuré de manière à en faciliter l'accès de diverses manières (p. ex. à l'aide de commandes spécifiques). De nombreuses méthodes et outils de cybersécurité visent à empêcher la perte ou la violation de données.
Bien-être numérique	État de santé mentale et physique d'une personne relativement à son utilisation d'Internet. La navigation et les interactions sur le web peuvent contribuer ou nuire au bien-être numérique d'une personne.
Bourrage d'identifiants	Type de cyberattaque qui consiste à entrer automatiquement sur de multiples plateformes des noms d'utilisateur et mots de passe piratés ou achetés afin de tenter d'accéder frauduleusement à des comptes d'utilisateur.
Cheval de Troie	Logiciel malveillant dissimulé à l'intérieur d'un logiciel inoffensif.

Terme	Définition
Chiffre de César	Une méthode simple de chiffrement qui consiste à décaler les caractères d'un texte d'un nombre déterminé de positions dans l'alphabet. Ce nombre de positions constitue la « clé » de chiffrement et sert aussi au déchiffrement. Exemple : La phrase « bcd » chiffrée à l'aide d'une clé de 1 décalage devient « abc ». Pour déchiffrer la phrase, il faut décaler les caractères dans le sens inverse indiqué par la clé.
Chiffrement ou cryptage	Opération qui consiste à encoder un message afin qu'il soit impossible à lire, sauf par la ou les personnes qui possèdent la clé pour le déchiffrer.
Citoyenneté numérique	Capacité à comprendre et à utiliser Internet de manière sûre et appropriée, ce qui requiert une connaissance de la **sécurité numérique**, de la **nétiquette** et du **bien-être numérique**.
Commerce électronique ou commerce en ligne	Ensemble des activités commerciales effectuées sur Internet, y compris la vente et l'achat de biens et de services. Comprend aussi souvent la livraison à domicile.
Communication numérique	Capacité à transmettre et à recevoir de l'information au moyen d'Internet quasi instantanément, peu importe la distance physique.
Confidentialité	Ce qui protège votre identité et vos renseignements contre la divulgation et l'accès non autorisés.
Cryptographie	Processus par lequel un texte écrit en clair est converti en code sécurisé, déchiffrable uniquement par la personne à laquelle il est destiné.
Cyberfuté	Une personne cyberfutée connaît suffisamment bien l'informatique et Internet pour exercer sa citoyenneté numérique avec confiance et naviguer sur le web de manière sûre et appropriée.

Terme	Définition
Cyberintimidation	Forme d'intimidation exercée uniquement en ligne et qui a des effets très néfastes sur la santé mentale de la victime.
Cybersécurité	Comme la sécurité à domicile, la cybersécurité a pour but d'empêcher les intrusions. La différence, c'est que la cybersécurité protège l'information numérique. Il existe une multitude de techniques et d'outils de cybersécurité. Voir aussi **sécurité numérique**.
Déchiffrement ou décryptage	Action qui consiste à déchiffrer un message afin que son destinataire puisse le lire.
Données personnelles ou renseignements personnels	Information confidentielle, associée exclusivement à une personne. Comprend les données personnelles d'identification, comme le NAS et le numéro de téléphone, et d'autres renseignements personnels, comme le dossier médical, les habitudes d'achat, la date de naissance et le genre.
Digital Health and Wellness	The physical and mental wellbeing of an individual with regards to the internet. Online interactions and information can either improve or detract from digital health.
Droits et responsabilités numériques	Terme qui désigne les droits fondamentaux en matière d'accès aux technologies et à Internet ainsi que les responsabilités à l'égard de l'utilisation sûre et appropriée de ceux-ci.
Ère numérique	Marquée par l'avènement des appareils mobiles connectés au début des années 2000, l'ère numérique (aussi appelée « ère d'Internet ») désigne une période de l'histoire durant laquelle Internet est devenu accessible au plus grand nombre et a commencé à exercer une fonction sociale.
Fausses nouvelles	Mésinformations diffusées intentionnellement afin de tromper les gens et d'en tirer un bénéfice financier ou politique.

Terme	Définition
Hachage	Méthode de cryptage à sens unique utilisée par les sites web et les applications afin de protéger des informations sensibles, comme les mots de passe. Chaque information sensible est associée à un code unique dont le site web ou l'application se sert pour l'authentifier.
Hameçonnage	Forme de fraude psychologique qui consiste à tromper une personne afin qu'elle divulgue volontairement ses renseignements personnels. **Exemple** : Vous recevez un courriel urgent d'un expéditeur inconnu vous demandant de cliquer sur un lien pour entrer vos identifiants sur la plateforme de l'école.
Hypertrucage (deepfake)	Procédé qui consiste à créer de toutes pièces des représentations audio ou vidéo très convaincantes de gens à des fins trompeuses.
Imposteur	Personne qui se fait passer pour quelqu'un d'autre ou qui tient des propos mensongers généralement dans le but de commettre une fraude.
Littératie numérique	Capacité à comprendre et à utiliser les technologies et Internet, ainsi qu'à créer et analyser de l'information en ligne en faisant preuve de jugement critique.
Logiciel antivirus	Logiciel conçu pour accéder à un ordinateur sans le consentement de son propriétaire afin d'y voler, altérer ou détruire des données. **Exemples** : virus, ver, rançongiciel, cheval de Troie, etc.
Mémoire	Dispositif de stockage de l'information enregistrée dans un ordinateur. Il existe plusieurs types de supports de mémoire, mais le plus courant est le disque dur.
Menace informatique ou cybermenace	Tout événement en ligne susceptible de mener à un méfait ou à un vol de données.

Terme	Définition
Mésinformation	Information fausse ou inexacte.
Nétiquette	Dérivé du mot « étiquette », qui désigne les règles à suivre pour bien se comporter dans certaines situations. La nétiquette renvoie donc aux règles à suivre pour bien se comporter en ligne.
Parti pris	Opinion préconçue servant à appuyer ou à rejeter quelqu'un ou quelque chose de manière injustifiée. Les partis pris d'une personne sont souvent sur des expériences antérieures, qu'elle a jugées bonnes ou mauvaises.
Piège à clics	Lien hypertextuel formulé de manière volontairement accrocheuse. Ces liens mènent généralement à des sites sans substance et truffés de publicités pouvant contenir des virus. **Exemple** : Vous ne croirez pas ce qu'a fait cette vedette!
Rançongiciel	Type de logiciel malveillant qui chiffre le contenu d'un ordinateur dans le but d'extorquer de l'argent à l'utilisateur. **Exemple** : On vous demande de payer 500 $ pour retrouver l'accès aux photos qui se trouvent sur votre ordinateur.
Réseau privé virtuel (RPV)	Selon Kapserky (s. d.), « un RPV établit une connexion sécurisée entre vous et Internet en acheminant tout votre trafic de données par un tunnel virtuel chiffré. Lorsque vous naviguez sur Internet à partir d'un RPV, votre adresse IP est dissimulée et votre ordinateur est à l'abri des attaques externes (traduction libre) ».
Sauvegarde de données	Opération qui consiste à copier sur un support informatique externe (clé USB, disque optique, disque dur externe, etc.) ou dans le nuage les données mises en mémoire afin de permettre leur restauration en cas de suppression ou de corruption.

Terme	Définition
Sécurité numérique	Protection de l'information se trouvant sur Internet et ensemble des mesures visant à empêcher des personnes malveillantes de voler ou utiliser cette information. Voir aussi **cybersécurité**.
Serveur	Pièce d'équipement informatique qui sert de point d'accès et de système de gestion pour d'autres ressources. **Exemple** : Un serveur de jeu vous permet de jouer à Minecraft avec vos amies et amis et un serveur web, d'accéder à des pages web.
Ver	Type de logiciel malveillant capable de s'exécuter et de se reproduire par lui-même afin de causer le plus dommages possibles.
Virus	Programme informatique aux effets nuisibles qui peut se répandre dans un réseau en se répliquant. Parmi les effets nuisibles, on trouve l'affichage de messages importuns, le vol de données ou la prise de contrôle de l'ordinateur.
Vulnérable (appareil ou réseau)	Qualifie un appareil ou un réseau informatique exposé à des cybermenaces. La vulnérabilité est souvent causée par l'absence de dispositifs de sécurité tels qu'un coupe-feu ou un antivirus.
Vulnérable (personne)	Qualifie les personnes sensibles aux arnaques en ligne et aux tentatives d'hameçonnage. Ces personnes sont moins familières avec Internet et ne savent pas comment y naviguer de façon sécuritaire.

Remerciements

Nous tenons à exprimer notre gratitude à nos conseillères, réviseures et collaboratrices:

- **Abbey Ramdeo,** Actua
- **Caitlin Quarrington,** Actua
- **Cat Coode,** Binary Tattoo
- **Emily Hartman,** Actua
- **Emily N. Cyr,** Université de Waterloo

Nous sommes aussi reconnaissantes et reconnaissants envers les nombreuses personnes au sein de **Femmes et Égalité des genres Canada**, d'**Enbridge** et de la **Fondation Motorola Solutions** qui nous ont fourni des commentaires précieux pour la mise en forme de ce projet.

De plus, nous voulons remercier les organismes membres de notre réseau, en particulier ceux qui ont contribué à la mise en œuvre du projet dans leur collectivité :

- **Memorial Engineering Outreach,** Université Memorial
- **Minds in Motions,** Université de Calgary
- **Science Venture,** Université de Victoria
- **SuperNOVA,** Université Dalhousie
- **Worlds UNBound,** Université du Nouveau-Brunswick

Et bien sûr, nous remercions tous les clubs BGC Canada qui ont participé au projet pilote.