La présence en ligne

5e à la 7e année

Actua | 111 Murray Street, Ottawa, ON K1N 5M5 | www.actua.ca | 613 234 4137

actüa
Jeunesse · STIM · Innovation
Youth · STEM · Innovation

La présence en ligne

Conditions d'utilisation

Avant de réaliser cette activité en tout ou en partie, vous reconnaissez et acceptez ce qui suit :

- il vous appartient de passer en revue toutes les sections du présent document et la documentation connexe ainsi que d'appliquer les consignes de sécurité nécessaires à la protection de toutes les personnes concernées;
- les mesures précisées à la rubrique « Consignes de sécurité » du présent document ne sont pas exhaustives ni ne remplacent votre propre cadre d'examen de la sécurité;
- Actua n'est pas responsable des dommages attribuables à l'usage du présent contenu;
- Vous pouvez adapter ce document à vos besoins (le remanier, le transformer ou créer du matériel à partir de celui-ci), à condition d'indiquer qu'Actua en est l'auteur original et que vous y avez apporté des changements. Ce contenu ne peut être transmis à de tierces parties sans la permission écrite d'Actua.

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, 350 000 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 actua.ca et suivez-nous sur Twitter, Facebook, Instagram et YouTube!

La présence en ligne

Présentation de l'activité

Les élèves vont explorer leur identité en ligne (et la façon dont celle-ci se compare à leur identité hors ligne) ainsi que réfléchir aux diverses intentions des autres utilisateurs et utilisatrices du web. Il sera notamment question de personnalité numérique et de surpartage. Cette activité permettra aux jeunes de mieux interpréter les comportements des autres dans le cyberespace et de prendre conscience de l'importance de leur empreinte numérique.

Cette activité fait partie d'une série d'activités basées sur l'éducation cybernétique. La suite comprend : La citoyenneté numérique et toi, La présence en ligne, Cyberdétective, La nétiquette, Craque le code et Sécurise ton réseau. Explorez le Guide pédagogique pour former des jeunes cyberfutés pour apprendre comment vous pouvez introduire l'éducation cybernétique dans votre milieu éducatif.

Activité conçue par Actua, 2022.

Environnement	Durée	Public cible	Spécifications techniques
En personne	1 h	5e-7e année *(10-13 ans)*	Certains exercices nécessitent l'utilisation d'un ordinateur portable ou d'une tablette. Moyennant certaines modifications, on peut regrouper les élèves en équipes de deux ou plus. **Les responsables de l'animation doivent avoir à leur disposition un ordinateur portable, un projecteur, des haut-parleurs et un écran ou un mur vierge pour y faire des projections.** • Projecteur • Haut-parleurs

Environnement	Durée	Public cible	Spécifications techniques
			• Écran ou mur vierge • Ordinateurs portables ou tablettes

Résultats d'apprentissage

À la fin de l'activité, les élèves sauront :

- interpréter les comportements en ligne;
- utiliser et transmettre à d'autres les principales stratégies pour fréquenter le cyberespace de manière futée et responsable;
- reconnaître le type d'information à ne pas publier sur Internet ainsi qu'éviter le surpartage de données personnelles (gestion des renseignements personnels).

OUTILS	COMPÉTENCES	ATTITUDES
Connaissances, ressources et expériences • Identité en ligne • Citoyenneté numérique • Médias sociaux • Empreinte numérique	**Compétences numériques et en STIM, et aptitudes essentielles à l'employabilité et à la vie quotidienne** • Littératie numérique • Comportement sûr et responsable en ligne • Communication en ligne	**Intelligence numérique, action communautaire et pensée computationnelle** • Compréhension de sa relation avec la technologie • Gestion des renseignements personnels

Logistique (durée, taille du groupe, matériel)

Section	Durée estimée	Taille du groupe	Matériel
Introduction	5 min	*Tout le groupe*	**Responsable de l'animation** • Tableau et marqueur
1. La personnalité numérique	25 min	*Tout le groupe*	**Par élève** • Ordinateur portable ou tablette • Avatar Google Sheets OU Feuille d'activité – Création d'un avatar (voir l'annexe C)
2. Le surpartage	25 min	*Tout le groupe; individuellement*	**Responsable de l'animation** • Teen Voices: Oversharing and Your Digital Footprint (sous-titres en français) • Tableau et marqueur **Par élève** • Ordinateur portable ou tablette • Faire de nouvelles rencontres (un jeu dont vous êtes le héros)
Réflexion et récapitulation	5 min	*Tout le groupe*	• S. O.

Consignes de sécurité

Les consignes de sécurité ci-dessous ne sont pas exhaustives. Veillez à passer en revue l'activité et à inspecter l'environnement où elle sera réalisée afin de déterminer

si des mesures additionnelles sont requises pour assurer la sécurité des élèves.

Sécurité émotionnelle

Ce projet vise à fournir aux jeunes les outils et les connaissances nécessaires pour comprendre les comportements en ligne et prendre des décisions sécuritaires.

- Tenez compte du fait que les élèves n'ont pas toutes et tous les mêmes expériences et connaissances en matière de pratiques cybersécuritaires, de cybersécurité et de citoyenneté numérique. La présente activité pourrait vous amener à discuter de sujets délicats, comme la cyberintimidation et d'autres cyberrisques. Veuillez préserver en tout temps la sécurité émotionnelle des jeunes et vous reporter à la formation reçue à votre établissement et pour ce projet.
- Orientez la discussion vers les comportements sains et sûrs en ligne et encouragez les jeunes à faire des choix responsables, informés et judicieux.

Sécurité en ligne

Certains volets de cette activité nécessitent l'usage d'appareils connectés à Internet.

- Examinez au préalable les vidéos, les sites web et le matériel prévus afin de vous assurer qu'ils conviennent à vos élèves.
- Au besoin, rappelez aux jeunes de se concentrer sur la tâche à faire et d'utiliser uniquement les liens fournis pour l'activité.
- Donnez l'exemple et encouragez l'adoption de comportements appropriés en ligne (poser des questions et y répondre dans la boîte de clavardage, employer un langage positif et motivant, utiliser les appareils uniquement pour réaliser l'activité, etc.).

Liens avec le programme d'études

Chacune des activités s'aligne avec ces trois aspects du Cadre de référence pancanadien pour l'enseignement de l'informatique :

Ordinateurs et réseaux : Cybersécurité

- L'élève débutant devrait pouvoir définir le concept de cybersécurité et

créer des mots de passe sûrs selon des critères d'efficacité. L'élève compétent devrait pouvoir décrire des types courants de cyberattaques et reconnaître le contenu malveillant, appliquer des moyens de prévention et évaluer le rôle joué par les personnes dans la création, la prévention et la réduction de la portée des cyberattaques ainsi que leurs effets sur la population et la société (p. 24).

Données : Gouvernance des données

- L'élève débutant devrait pouvoir nommer des manières dont les activités numériques ou physiques créent des données numériques et régler les paramètres de confidentialité sur des outils numériques couramment utilisés. L'élève compétent devrait pouvoir déterminer qui possède ses données numériques, évaluer les lois et les politiques provinciales et fédérales sur la gouvernance des données et les accords autochtones sur la gouvernance des données et comprendre, ainsi que défendre ses droits par rapport aux données et ceux des autres (p. 26).

Technologie et société : Éthique, sécurité et politique

- L'élève débutant devrait pouvoir décrire des stratégies pour protéger ses renseignements personnels et son identité en ligne. L'élève compétent devrait pouvoir définir et appliquer des principes de base en lien avec les droits d'auteur, expliquer les problèmes liés à la vie privée et évaluer les effets de la cybercriminalité et du piratage sur soi-même et la société (p. 28).

Marche à suivre

Préparation

Section	Préparation

Généralités	• **Préparez l'activité et les mesures d'adaptation requises, s'il y a lieu :**
	  ○ Déterminez votre **mode d'enseignement** et puisez des idées, au besoin, dans les sections Recommandations selon le mode d'enseignement et Possibilités d'adaptation.
	  ○ Même si la **durée estimée** est précisée, il peut être utile de réfléchir au temps que vous voulez consacrer aux différents exercices et aux discussions.
	  ○ La **taille du groupe** indiquée (en équipes de deux ou plus, ou individuellement) n'est qu'une suggestion et peut être adaptée aux besoins de votre classe.
	• **Contenu :**
	  ○ **Préparez des réponses** aux diverses questions de réflexion posées durant l'activité.
	  ○ Examinez les vidéos et le matériel fournis à l'annexe C pour déterminer si leur contenu **convient** à vos élèves.
	• **Matériel :**
	  ○ Vérifiez que votre appareil, l'écran et le projecteur sont bien installés et fonctionnels.
	  ○ Préparez les appareils des élèves.

Section	Préparation
1. La personnalité numérique	• Déterminez la meilleure méthode pour créer un avatar à partir des ressources disponibles et du mode d'enseignement retenu. ○ Selon l'approche choisie, prenez connaissance de l'avatar dans Google Sheets, Excel ou la feuille d'activité.
2. Le surpartage	• Familiarisez-vous avec le jeu dont vous êtes le héros Faire de nouvelles rencontres.

Introduction

1. Demandez aux élèves de deviner la moyenne d'heures passées en ligne chaque jour par une personne de moins de 25 ans. Réponse : environ 7 heures!
2. Démarrez un remue-méninges en notant au tableau les réponses des élèves à la question suivante : **« Selon vous, comment les gens passent-ils ces heures en ligne? Être en ligne, en quoi ça consiste pour vous? »**
    1. *Autres amorces* : Que faites-vous en ligne? Qu'est-ce que vous pouvez faire sur Internet?
    2. *Réponses possibles : Utiliser Google Classroom pour apprendre, jouer à des jeux, apprendre à coder sur Scratch, jouer sur ma console Switch, regarder des vidéos sur YouTube, visionner des films sur Netflix, faire des recherches.*

1. La personnalité numérique

1. En ligne, un **avatar** (ou image de profil) est une représentation virtuelle d'une utilisatrice ou d'un utilisateur ou de sa personnalité. Donnez aux élèves 10 minutes pour personnaliser le modèle d'avatar fourni dans le document Avatar Google Sheets en sélectionnant la couleur de chaque pixel. Les jeunes peuvent modifier l'avatar à leur guise (représentation d'eux-mêmes,

personnage tiré de leur film préféré, personnage imaginaire, etc.).

a. ***Remarque :*** Cette activité peut être réalisée de plusieurs façons :
    i. Vous pouvez imprimer la Feuille d'activité – Création d'un avatar afin que les élèves puissent la colorier (voir l'annexe C).
    ii. Les jeunes peuvent modifier le modèle d'avatar fourni dans le document Avatar Google Sheets.
        1. Pour faire une copie du modèle en vue de le modifier, il faut disposer d'un compte Google. Autrement, on peut copier l'onglet principal et l'enregistrer sous un autre nom.
            a. Si les jeunes ne connaissent pas Google Sheets, offrez-leur un court tutoriel (sélectionner la couleur de plusieurs cellules à la fois, sélectionner la couleur d'une seule cellule, modifier la couleur, enregistrer une copie du document, copier un onglet, etc.).
    iii. Vous pouvez télécharger le document et le transmettre aux élèves sous forme de fichier Excel. Si vous optez pour ce format, prévoyez un tutoriel sur l'utilisation d'Excel.

2. Animez une discussion à partir des questions suivantes :
    a. **« Comment avez-vous personnalisé votre avatar? Pourquoi lui avez-vous donné cette allure? »**
        i. ***Remarque :*** *Prévoyez une méthode permettant aux jeunes de présenter leur avatar à leurs collègues, s'ils et elles sont à l'aise avec cela.*
    b. **« Croyez-vous que la représentation virtuelle des gens corresponde toujours à ce qu'ils sont en personne? Comment cela peut-il influencer la façon dont les gens interagissent en ligne?"**
        i. *Réponses possibles : En ligne, certaines personnes peuvent être plus à l'aise d'être elles-mêmes et de dire ce qu'elles pensent vraiment (surtout si elles sont anonymes); d'autres peuvent se présenter sous une fausse identité pour tromper quelqu'un (pour devenir leur ami, pour voler de l'information, etc.).*
        ii. ***Remarque :*** La discussion peut prendre un tour plus sérieux ici.

Insistez sur le fait qu'il ne faut pas seulement porter attention à qui on est en ligne, mais aussi à qui sont les autres.

2. Le surpartage

1. On peut faire du surpartage hors ligne et en ligne. Posez cette question aux jeunes : **« Comment définiriez-vous le surpartage? »** (Pour en savoir plus, voir l'annexe B, Information documentaire.)
2. Montrez cette vidéo : Teen Voices: Oversharing and Your Digital Footprint (Common Sense Education, 3:34, sous-titres en français).
    a. ***Remarque* :** Même si certains élèves ne publient pas encore de contenu en ligne, elles et ils doivent savoir ce qu'est le surpartage en prévision de l'avenir.
3. Démarrez un remue-méninges en notant au tableau les réponses des élèves à la question suivante : **« Quels types de renseignements devriez-vous garder confidentiels (hors ligne ET en ligne)? »**
    a. ***Remarque* :** Ajoutez les éléments suivants à la liste s'ils n'ont pas été mentionnés par les élèves :
        i. Nom et prénom, adresse courriel, sport préféré, nom de l'école, noms des parents, date de naissance, situation de couple (et d'autres exemples de données personnelles pouvant servir à identifier une personne).
4. Posez ensuite cette question : **« Quels sont les risques du surpartage? »**
    a. *Réponses possibles :* *Nos renseignements pourraient être volés (date de naissance, localisation, nom et prénom, etc.); de faux comptes pourraient être créés à partir de notre profil; des recruteurs pourraient voir des choses embarrassantes à notre sujet qui pourraient nuire à nos chances d'être admis dans une école ou d'obtenir un emploi; le surpartage entre amis peut causer de la rancœur et un sentiment de trahison.*
    b. ***Remarque* :** Certaines réponses peuvent concerner des sujets plus sérieux, comme le kidnappage et le harcèlement. Insistez sur l'importance de prendre garde à ce qu'on partage en ligne et avec qui.

5. Invitez les élèves à jouer pendant 10 minutes à Faire de nouvelles rencontres (un jeu dont vous êtes le héros créé avec Twine et hébergé sur Itch.io). Le but du jeu consiste à prendre les décisions les plus cyberfutées parmi les options proposées dans l'histoire (une personne inconnue envoie des messages au personnage principal qui joue en ligne).
    a. ***Remarque* :** Les jeunes peuvent jouer individuellement ou en équipes de deux ou plus.
6. Posez cette question aux élèves : **« Si vous interagissez en ligne avec une personne qui vous met mal à l'aise (p. ex., pendant un jeu, dans les commentaires YouTube, etc.), que pouvez-vous faire? »**
    a. *Réponses possibles :* *On signale le compte* (toutes les plateformes de médias sociaux proposent des moyens de signaler un compte anonymement, c'est-à-dire sans que le propriétaire du compte sache qu'on l'a signalé)*; si on connaît la personne, on vérifie de vive voix que c'est bien elle qui a communiqué avec nous; on en parle à une ou un adulte en qui on a confiance (*parent, tutrice ou tuteur, enseignante ou enseignant, etc.*); on ignore la personne et on ne lui répond pas; on bloque ou on met en sourdine la personne; on fait une capture d'écran du message pour garder une preuve de l'imposture; on active les paramètres de confidentialité de tous nos comptes.*

Réflexion et récapitulation

1. Abordez les questions ci-dessous avec les élèves pour les amener à réfléchir à leurs comportements et à leurs expériences en ligne (discussion avec toute la classe ou en petits groupes, ou réflexion individuelle) :
    a. **« Comment compareriez-vous votre identité hors ligne et en ligne? »**
    b. **« D'après vous, pourquoi est-il important de se concentrer sur les interactions en personne, et pas seulement sur les interactions virtuelles? »**
2. Discutez des différentes professions présentées à l'annexe A, Liens avec des professions.
3. Encouragez les élèves à devenir des ambassadrices et des ambassadeurs

cyberfutés en transmettant à leur famille et à leurs amis les stratégies apprises durant cette activité.

Recommandations selon le mode d'enseignement

Ce contenu a été conçu pour l'enseignement en personne, mais peut être présenté dans d'autres contextes. Voici des recommandations pour l'enseigner à distance (en ligne) ou dans un environnement « débranché » (avec peu ou pas de support technologique).

<table>
<tr><th>À distance (en ligne)</th><th>Débranché (peu ou pas de techno)</th></tr>
<tr><td colspan="2">Généralités</td></tr>
<tr><td>Invitez les jeunes à ouvrir leur micro ou à utiliser la boîte de clavardage, à leur convenance.
Utilisez un outil permettant à tous les élèves de participer aux discussions en ligne (Mentimeter, Jamboard, etc).
Notez les liens à fournir aux élèves et copiez-les dans la boîte de clavardage au moment opportun.
Faites appel à des sondages ou à d'autres formes d'interactions en groupe pour faire le point avec les élèves et maintenir leur niveau de motivation.</td><td>Utilisez un tableau pour faire des remue-méninges et noter les idées et réponses des jeunes.</td></tr>
<tr><td colspan="2">Introduction</td></tr>
</table>

À distance (en ligne)	Débranché (peu ou pas de techno)
• L'exercice peut être réalisé tel quel en ligne. Le remue-méninges peut se faire verbalement ou au moyen d'un outil de collaboration (Jamboard, Google Doc, Mentimeter, etc.).	• L'exercice peut être réalisé tel quel, sans support technologique.
1. La personnalité numérique	
• Utilisez le document Google Sheets. ***Remarque :*** Pour pouvoir modifier le document, les élèves devront en faire une copie. Pour ce faire, elles et ils devront disposer d'un compte Google ou copier l'onglet et l'enregistrer sous un autre nom.	• Imprimez la Feuille d'activité – Création d'un avatar (voir l'annexe C) et demandez aux jeunes de colorier leur avatar (voir aussi les autres ressources ci-dessous).
2. Le surpartage	
• L'exercice peut être réalisé tel quel en ligne. Le remue-méninges peut se faire verbalement ou au moyen d'un outil de collaboration (Jamboard, Google Doc, Mentimeter, etc.).	• Plutôt que d'utiliser l'histoire créée avec Twine, rédigez des scénarios sur le surpartage et distribuez-les aux élèves répartis en équipes. Demandez à chaque équipe de concevoir sa propre histoire sur le surpartage à partir du scénario reçu

À distance (en ligne)	Débranché (peu ou pas de techno)
	(chaque histoire devrait comporter des décisions cyberfutées).
Réflexion et récapitulation	
• L'exercice peut être réalisé tel quel en ligne. Le remue-méninges peut se faire verbalement ou au moyen d'un outil de collaboration (Jamboard, Google Doc, Mentimeter, etc.).	• L'exercice peut être réalisé tel quel, sans support technologique.

Possibilités d'adaptation

Il est possible d'adapter différents aspects de cette activité (durée, environnement, matériel, taille du groupe ou instructions) pour la rendre plus accessible ou plus complexe. Les **modifications** ci-dessous vous permettront de diminuer le niveau de difficulté de l'activité et les **ajouts**, d'augmenter sa durée ou son niveau de difficulté.

Modifications

GÉNÉRALITÉS

- Sélectionnez l'option de sous-titrage (si disponible) pour la diffusion des vidéos.
- Fournissez une souris aux jeunes pour faciliter l'utilisation de l'ordinateur portable.
- Faites travailler les élèves en équipes de deux ou plus plutôt qu'individuellement.

1. LA PERSONNALITÉ NUMÉRIQUE

- Distribuez une version imprimée de la Feuille d'activité – Création d'un avatar et demandez aux élèves de colorier l'avatar.

2. LE SURPARTAGE

- Jouez à Band Runner - Think U Know (en anglais) plutôt qu'à Faire de nouvelles rencontres. Band Runner comprend de la musique et permet d'accumuler des points. Son but est semblable, soit de se familiariser avec la sécurité en ligne en aidant les personnages à prendre des décisions cyberfutées.
- Jouez à Faire de nouvelles rencontres avec toute la classe en lisant l'histoire à haute voix.

Ajouts

GÉNÉRALITÉS

- **Lien avec l'informatique :** Lancez une discussion à propos de l'intelligence artificielle **(p. ex. sur les bots ou robots logiciels).**
    - Sur des plateformes comme Twitter, de nombreux comptes sont administrés par des « bots », des robots logiciels programmés pour imiter les capacités d'un être humain dans un système informatique. Les bots utilisent des photos tirées d'Internet et génèrent du contenu.
    - Avez-vous déjà interagi avec des bots? Ceux-ci tendent à réutiliser ou à republier de l'information provenant d'ailleurs et fournissent très peu de détails personnels.

1. LA PERSONNALITÉ NUMÉRIQUE

- Montrez aux élèves des exemples tirés d'une série du New York Times présentant des photos d'utilisateurs avec leur avatar. Explorez avec les jeunes les raisons pour lesquelles certaines personnes pourraient vouloir adopter une personnalité différente en ligne. Examinez les images au

préalable afin de sélectionner celles qui sont appropriées pour vos élèves. Pour passer d'une image à l'autre, cliquez sur les boutons Next/Previous (Suivante/Précédente) dans le coin supérieur droit.

2. LE SURPARTAGE

- Faites le jeu Fight Back: Battle the Werewolf (volet d'une série de jeux en ligne de Texas A&M Information Technology permettant aux jeunes de tester leurs connaissances et comportements en matière de sécurité en ligne).
- Avec les élèves, analysez le profil de différentes vedettes et voyez ce qu'il est possible de découvrir à leur sujet en six clics. (6 Degrees of Information, sous-titres en français)
- Discutez des *raisons* pour lesquelles les gens partagent trop d'information en ligne : CBC - Your brain on likes: The science of oversharing online (en anglais).

RÉFLEXION ET RÉCAPITULATION

- Les élèves peuvent créer une affiche avec Canva afin de faire connaître à leurs amis et à leur famille les pratiques cybersécuritaires à adopter lorsqu'on interagit avec de nouvelles personnes en ligne. Transmettez-leur ce lien utile https://www.canva.com/fr_fr/affiches/modeles/campagne-affichage/ et explorez vous-même toutes les possibilités de cet outil.
    - Montrez rapidement aux jeunes comment créer et personnaliser un projet dans Canva. Si cela facilite l'activité, sélectionnez vous-même un modèle sur la plateforme plutôt que de laisser ce choix aux élèves ou de les laisser dessiner leur propre affiche.
    - Les élèves peuvent concevoir leur affiche sur papier plutôt que d'utiliser Canva.
    - Si le temps le permet, invitez les élèves à présenter leur affiche à la classe.

Références et remerciements

Centre canadien pour la cybersécurité. (3 juillet 2020). *Faux comptes de médias sociaux*. https://cyber.gc.ca/fr/orientation/faux-comptes-de-medias-sociaux

Commissariat à la protection de la vie privée du Canada. (23 janvier 2020). *Vos amis sont-ils bien ceux qu'ils prétendent?* https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/campagnes-et-activites-de-sensibilisation/sensibilisation-des-enfants-a-la-vie-privee/fs-fi/friend-ami/

Commissariat à la protection de la vie privée du Canada. (10 janvier 2018). *Sujet de discussion no 7 : Usurpation d'identité en ligne – empêchez les gens de détourner votre compte et de se faire passer pour vous.* https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/campagnes-et-activites-de-sensibilisation/sensibilisation-des-enfants-a-la-vie-privee/topic-sujet/dt_07/

Common Sense Education. (12 janvier 2019). *Teen Voices: Oversharing and Your Digital Footprint* [Vidéo]. https://www.youtube.com/watch?v=ottnH427Fr8

Cyber Degrees. (9 avril 2020). *How to Become a Security Software Developer*. https://www.cyberdegrees.org/jobs/security-software-developer/

Gouvernement du Canada. (25 août 2020). *Analyste du renseignement sur la cybercriminalité* [Offre d'emploi]. https://emploisfp-psjobs.cfp-psc.gc.ca/psrs-srfp/applicant/page1800?toggleLanguage=fr&poster=1449726

Gouvernement du Canada. (s. d.). *Réseaux sociaux (Pensez cybersécurité)*. https://www.pensezcybersecurite.gc.ca/fr/securisez-vos-comptes/reseaux-sociaux

Rasmussen College. (1er octobre 2018). *Everything You Need to Know About Becoming a Cyber Security Analyst*. https://www.rasmussen.edu/degrees/technology/blog/becoming-cyber-security-analyst/

Texas A&M University. (s. d.). *7 Tips for Safe Social Networking*. https://it.tamu.edu/security/safe-computing/identity/safe-social-networking.php

University of San Diego. (s. d.). *Master of Science in Cyber Security*. https://onlinedegrees.sandiego.edu/should-you-become-a-cyber-security-engineer/

U.S. Army Cyber Command. (13 février 2018). *Cybersecurity Fact Sheet: Social Media Imposters*. https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/1440824/cybersecurity-fact-sheet-social-media-impostors/

Viswanathan, Uma. (6 mai 2021). *Stay safe on social.* McGill University. https://www.mcgill.ca/cybersafe/article/stay-safe-social

Annexes

Annexe A : Liens avec des professions

GENDARMERIE ROYALE DU CANADA : ANALYSTE DE RENSEIGNEMENTS EN CYBERCRIMINALITÉ

- L'analyste de renseignements en cybercriminalité élabore des stratégies pour cerner les types de cybercrimes et les tendances en la matière. Elle ou il utilise cette information pour concevoir des outils de renseignement stratégique et pour fournir son avis lors d'enquêtes criminelles complexes.

SPÉCIALISTE EN CYBERSÉCURITÉ (SPÉCIALISTE EN SÉCURITÉ DE L'INFORMATION)

- La ou le spécialiste en cybersécurité repère les vulnérabilités des systèmes informatiques et des logiciels ainsi que les menaces visant ceux-ci. Elle ou il élabore des mesures de sécurité et des solutions afin de protéger les systèmes contre les cybercrimes tels que le piratage et les logiciels malveillants. Ces mesures et solutions peuvent prendre la forme de technologies ou de processus organisationnels.

ANALYSTE EN CYBERSÉCURITÉ (ANALYSTE EN SÉCURITÉ DE L'INFORMATION)

- L'analyste en cybersécurité surveille les réseaux et les systèmes informatiques d'une entreprise et protège ceux-ci contre les menaces et les brèches informatiques en élaborant et implantant des mesures de sécurité.

DÉVELOPPEUSE, DÉVELOPPEUR DE LOGICIELS DE SÉCURITÉ

- La développeuse ou le développeur de logiciels de sécurité conçoit et implante des outils de sécurité logicielle, développe des systèmes et teste la vulnérabilité de tous ces outils et systèmes.

Annexe B : Information documentaire

LE SURPARTAGE

Lorsque vous publiez du contenu dans les médias sociaux ou communiquez avec de nouvelles personnes en ligne, le surpartage (partager trop d'information) peut s'avérer risqué. Cela peut vous exposer aux vols d'identité et même mettre votre sécurité physique en danger. Il est recommandé de ne pas partager de données personnelles publiquement sur Internet.

Les données personnelles

Les données personnelles comprennent tous les renseignements à votre sujet. Certains de ces renseignements personnels peuvent être utilisés seuls ou en combinaison avec d'autres pour vous identifier. Exemples :

- Nom et prénom
- Adresse courriel
- Sport pratiqué
- Nom de l'école
- Nom du père
- Date de naissance
- Situation de couple

La plupart des gens savent que la divulgation de renseignements de carte de crédit présente un très grand risque. Cependant, saviez-vous qu'il est tout aussi risqué de publier une photo de soi en précisant où l'on se trouve? Il faut toujours garder cela en tête lorsqu'on partage du contenu en ligne, car on ne sait jamais qui se trouve de l'autre côté de l'écran (Stay Safe Online, 2021, en anglais).

Les risques du surpartage

- En indiquant votre emplacement publiquement ou à des étrangers, vous pourriez courir le risque :
    - de dévoiler à des criminels le lieu où vous vivez, étudiez ou travaillez;
    - de recevoir des courriels de harponnage (hameçonnage ciblé pour tenter de voler des renseignements sensibles);

- d'être victime d'un vol à domicile (si vous annoncez que vous êtes en voyage, on saura que vous avez laissé vos objets de valeur sans surveillance);
- d'être victime d'un vol d'identité ou d'un piratage de compte (vos renseignements personnels comme votre date de naissance ou votre lieu d'études peuvent servir à réinitialiser vos mots de passe si vous les avez aussi utilisés comme réponses à des questions d'identification).

Quelques bonnes pratiques cybersécuritaires

- Créez des mots de passe forts et uniques.
- Utilisez l'authentification à deux facteurs.
- Évitez de partager ce qui suit (Source : Gouvernement du Canada, Pensez cybersécurité, 2020) :
  - Renseignements personnels : numéro de téléphone, adresse courriel, adresse du domicile, lieu de travail ou d'études, etc.
  - Photos révélatrices : par exemple, un arrière-plan dévoilant le numéro de votre plaque d'immatriculation, le nom de votre rue, etc.
    - Photos géolocalisées : photos indiquant le lieu où elles ont été prises.
  - « Grandes » nouvelles : vacances, gros achats, événements à l'extérieur de la maison.
  - Information bancaire ou financière : nom de l'institution financière, numéro de carte, etc.
- Conseils pour utiliser les réseaux sociaux de façon sécuritaire (Source : Division of Information Technology, s. d.) :
  - Ne révélez jamais le lieu où vous vous trouvez.
  - Revoyez et ajustez vos paramètres de confidentialité régulièrement pour limiter la visibilité du contenu que vous partagez.
    - Agissez de façon prudente et responsable lorsque vous échangez avec d'autres personnes et partagez de l'information en ligne.

- Appliquez la règle du « futur moi » : Projetez-vous dans l'avenir et demandez-vous si votre futur moi aimerait votre publication. Imaginez que vous êtes parent, que vous soumettez une demande d'admission à l'université, que vous postulez un emploi ou que vous exercez une profession. Si la réponse est « non », vous ne devriez probablement pas publier cela.
    - Les employeurs, les entraîneurs et les gestionnaires d'établissements d'enseignement consultent les réseaux sociaux afin d'« apprendre à connaître » et de présélectionner les candidates et les candidats. Ne laissez pas des publications douteuses vous causer des problèmes dans l'avenir.
    - D'autres personnes pourraient aussi être affectées par ce que vous publiez, qu'il s'agisse de photos où elles figurent ou de vos commentaires à leur sujet.

LES IMPOSTEURS EN LIGNE

Les imposteurs en ligne sont des utilisateurs ou des utilisatrices qui prétendent être quelqu'un d'autre. Ils peuvent usurper l'identité d'une personne que vous connaissez et même la vôtre. Même si vous ne possédez pas de compte sur un réseau social, vous n'êtes pas à l'abri des imposteurs. Une personne pourrait voler vos renseignements personnels, créer un compte à votre nom et prétendre être elle-même la victime d'une imposture. Les intentions des imposteurs varient, mais plusieurs cherchent à ruiner la réputation de quelqu'un ou à tromper des gens afin d'obtenir des renseignements confidentiels ou personnels (Source : U.S. Army Cyber Command, 2018).

Méfiez-vous des messages étranges

1. L'expéditeur vous offre quelque chose de trop beau pour être vrai (p. ex. pour gagner 1 000 $, vous n'avez qu'à transmettre certains renseignements).
2. L'expéditeur vous demande de fournir des renseignements personnels.
3. L'expéditeur tente de vous convaincre de cliquer sur un lien (les liens peuvent servir à télécharger des applications indétectables afin de révéler votre

emplacement ou donner accès à votre appareil).

4. L'expéditeur vous propose de rencontrer certains de ses amis.

Que faire si vous croyez avoir affaire à un imposteur?

Selon le Centre canadien pour la cybersécurité, plusieurs plateformes sociales, comme Facebook, Twitter et Instagram, possèdent des mécanismes de signalement. Il est important de signaler tout compte qui vous semble frauduleux sur la plateforme où il se trouve.

Comment réduire votre vulnérabilité aux impostures dans les médias sociaux

Le gouvernement du Canada et la U.S. Army Cyber Command proposent les stratégies suivantes :

- Cherchez régulièrement votre nom sur les plateformes sociales, y compris en essayant diverses orthographes. Souvent, les imposteurs modifient légèrement le nom de la personne dont ils usurpent l'identité afin de ne pas être détectés.
- Revoyez régulièrement vos paramètres de confidentialité.
- Gardez confidentiels vos renseignements confidentiels.
- Faites preuve de prudence dans vos interactions en ligne.

Utilisez la fonction de recherche d'image inversée dans Google afin de chercher des photos publiques de vous et de vous assurer qu'elles n'ont pas été utilisées dans le profil d'un faux compte.

Annexe C : Autres ressources

1. LA PERSONNALITÉ NUMÉRIQUE

Feuilles d'activité

- Avatar Google Sheets
- Feuille d'activité – Création d'un avatar

2. LE SURPARTAGE

Vidéo

- Teen Voices: Oversharing and Your Digital Footprint (Common Sense Education, 3:34) (sous-titres en français)

Site web

- Faire de nouvelles rencontres (un jeu dont vous êtes le héros)

Feuille d’activité – Création d’un avatar

Un avatar est une représentation de toi-même dans un environnement virtuel (comme un jeu vidéo). Colorie les pixels ci-dessous pour créer ton avatar. Tu trouveras des exemples au bas de la page.