



La présence en ligne

8^e à la 12^e année

La présence en ligne

Conditions d'utilisation	3
À propos d'Actua	3
Présentation de l'activité	4
Résultats d'apprentissage	4
Logistique (durée, taille du groupe, matériel)	5
Consignes de sécurité	7
Liens avec le programme d'études	8
Marche à suivre	10
Préparation	10
Introduction	11
1. L'empreinte numérique	11
2. Qui sont les autres en ligne?	14
3. Le bien-être numérique	15
Réflexion et récapitulation	17
Recommandations selon le mode d'enseignement	17
À distance (en ligne)	18
Débranché (peu ou pas de techno)	18
Possibilités d'adaptation	20
Modifications	20
Ajouts	21
Références et remerciements	23
Annexes	25
Annexe A : Liens avec des professions	25
Annexe B : Information documentaire	26
Annexe C : Autres ressources	31

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 réfléchir aux diverses intentions des autres utilisateurs et utilisatrices du web. Il sera notamment question d'empreinte numérique, de médias sociaux, de surpartage et de bien-être numérique. Cette activité permettra aux jeunes de mieux interpréter les comportements des autres dans le cyberspace 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 netiquette, 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	1,75 h	8 ^e -12 ^e année (14-18 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 • Écran ou mur vierge

Environnement	Durée	Public cible	Spécifications techniques
			• Ordinateurs portables ou tablettes

Résultats d'apprentissage

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

- cerner leur empreinte numérique et interpréter les comportements des autres en ligne;
- utiliser et transmettre à d'autres les principales stratégies pour fréquenter le cyberspace 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);
- veiller à leur bien-être numérique.

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 • Bien-être numérique • Gestion des renseignements personnels

Logistique (durée, taille du groupe, matériel)

Section	Durée estimée	Taille du groupe	Matériel
Introduction	10 min	<i>Tout le groupe</i>	Responsable de l'animation • Tableau et marqueur Par élève • Ordinateur portable ou tablette
1. L'empreinte numérique	PARTIE 1 : La gestion de l'empreinte numérique 15 min	<i>Tout le groupe; individuelle ment</i>	Responsable de l'animation • Live My Digital for students: Digital Footprint (sous-titres en français) Par élève • Papier et crayon
	PARTIE 2 : Le surpartage 20 min	<i>Tout le groupe</i>	Responsable de l'animation • Teen Voices: Oversharing and Your Digital Footprint (sous-titres en français) • Tableau et marqueur • Présentation Le surpartage dans les profils de médias sociaux
	PARTIE 3 : Réflexion sur les	<i>Tout le groupe</i>	Responsable de l'animation • Exemple de carte d'une empreinte numérique

Section	Durée estimée	Taille du groupe	Matériel
	médias sociaux 15 min		• Tableau et marqueur
2. Qui sont les autres en ligne?	15 min	<i>Tout le groupe; individuelle ment</i>	Par élève • Ordinateur portable ou tablette • L'imposteur (un jeu dont vous êtes le héros)
3. Le bien-être numérique	20 min	<i>Tout le groupe; individuelle ment</i>	Responsable de l'animation • Présentation Mêmes sur le bien-être numérique • Logos de médias sociaux Par élève • Crayons de couleur et papier • Ordinateur portable ou tablette • Meta : Promouvoir la sécurité et la liberté d'expression • TikTok : Guide de bien-être
Réflexion et récapitulation	10 min	<i>Tout le groupe</i>	• 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 groupe. • 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
Section 1, partie 2 : Le surpartage	Prenez connaissance du contenu de la présentation Le surpartage dans les profils de médias sociaux.
Section 2 : Qui sont les autres en ligne?	Familiarisez-vous avec le jeu dont vous êtes le héros, L'imposteur.
Section 3 : Le bien-être numérique	Consultez les ressources en matière de bien-être et de sécurité numériques proposées par deux plateformes sociales populaires : Meta (Facebook, Instagram, WhatsApp, etc.) et TikTok.

Introduction

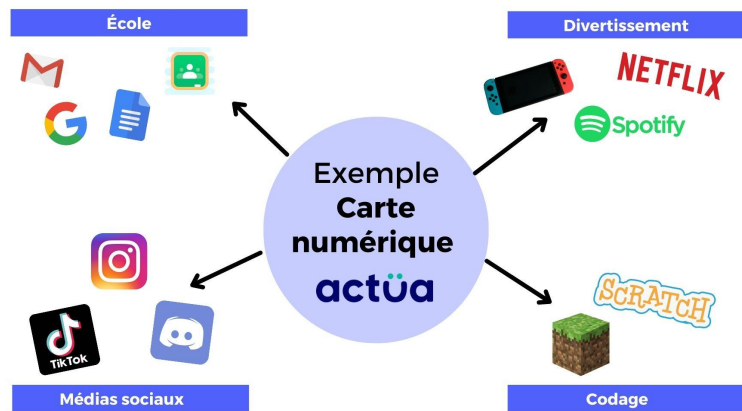
- Posez les questions suivantes :
 - « **Quelle est la dernière chose que vous avez publiée en ligne?** »
 - « **Que croyez-vous trouver si vous cherchez votre nom dans Google?** »
- Si cela convient au contexte et à vos élèves, demandez-leur de chercher leur nom dans Google pour voir le résultat. Chercher régulièrement son nom dans Google fait partie des bonnes pratiques de gestion de l'empreinte numérique.

1. L'empreinte numérique

PARTIE 1 : LA GESTION DE L'EMPREINTE NUMÉRIQUE

- 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!
- Démarrez un remue-méninges en notant au tableau les réponses des élèves à cette question : « **Passer du temps en ligne, en quoi ça consiste pour vous?** »
 - Autres amorces : Que faites-vous en ligne? Qu'est-ce que vous pouvez faire sur Internet?

- b. Réponses possibles : Consulter son fil d'actualité sur les médias sociaux, publier sur TikTok, regarder des vidéos sur YouTube, visionner des films sur Netflix, jouer à des jeux (p. ex. League of Legends, Minecraft), faire des appels vidéos aux amis, faire des recherches en ligne.
3. Demandez ceci aux jeunes : « **Que savez-vous à propos de l'empreinte numérique?** » Il s'agit de la trace de données laissée par vos actions sur Internet (vos consultations de sites web, vos publications, vos courriels, etc.).
4. Cartographie de l'empreinte numérique : Distribuez des feuilles de papier et des crayons aux élèves. Demandez-leur d'écrire leur nom au centre de la feuille et d'indiquer leurs diverses utilisations d'Internet dans la dernière semaine (voir l'exemple ci-contre).
- a. Si le temps le permet, demandez aux jeunes de comparer leur empreinte numérique avec celle d'une personne qui habite dans une région rurale ou éloignée où la connexion Internet est mauvaise.
5. [Live My Digital for students: Digital Footprint](#) (GDST, 4:52, sous-titres en français)



PARTIE 2 : LE SURPARTAGE

1. 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).
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 une équipe sportive, ou encore 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 kidnapping et le harcèlement. Insistez sur l'importance de prendre garde à ce qu'on partage en ligne et avec qui.
5. Présentez le contenu de [Le surpartage dans les profils de médias sociaux](#). Les élèves doivent examiner des profils publics et déterminer si ceux-ci contiennent des renseignements personnels susceptibles d'intéresser un cybercriminel (pour en savoir plus, voir les notes de présentation sous chaque diapo).
- a. Après chaque diapo, faites une discussion de groupe sur les renseignements pouvant intéresser un cybercriminel dans le profil présenté.
- b. Demandez aux jeunes de suggérer des stratégies pour rendre ces profils plus sécuritaires (moyens de prévention/mesures de sécurité).
- i. Réponses possibles : Rendre le compte privé (modifier les paramètres de confidentialité) – aucun de ces comptes n'est privé et certaines publications sont publiques; faire preuve de jugement lorsqu'on publie du contenu (penser à ce que sa grand-mère ou son futur moi penserait de cela); n'accepter que

des abonnés qu'on connaît; revoir régulièrement le contenu du profil.

- ii. Consultez l'annexe B, Information documentaire, pour en savoir plus.

PARTIE 3 : RÉFLEXION SUR LES MÉDIAS SOCIAUX

1. Demandez ceci aux jeunes : « **Qu'est-ce qu'un média social?** »
2. Affichez ces logos de médias sociaux et posez ces questions : « **Combien de ces médias sociaux connaissez-vous? Sur combien de ces médias sociaux avez-vous un compte? Qu'est-ce qui vous a donné envie d'avoir un compte sur ces médias sociaux ?** »

actüa

Exemples de médias sociaux



YouTube



Discord



Twitter



Pinterest



Snapchat



Tumblr



WhatsApp



Facebook



TikTok



LinkedIn

3. Faites un remue-méninges en groupe sur les avantages et les inconvénients des médias sociaux.
 - a. Réponses possibles (avantages): Permettent de rencontrer des gens de divers horizons, de trouver des groupes avec lesquels on a des affinités (p. ex. communautés LGBTQ+), de garder le contact, etc.
 - b. Réponses possibles (inconvénients): Entraînent les comparaisons, nuisent à la santé mentale, peuvent créer une dépendance, etc.
 - c. **Remarques** : Cette discussion peut être étendue afin d'amener les élèves à comparer deux types de comptes (p. ex. page de mèmes

[9GAG] par rapport à page éducative [National Geographic]) : Qui a créé ce contenu? Est-ce gentil? Quel type d'information y publie-t-on?

2. Qui sont les autres en ligne?

1. Posez cette question : « **Pourquoi une personne voudrait-elle changer partiellement ou complètement d'identité en ligne?** »

a. Réponses possibles : *Pour tromper des gens afin d'obtenir leurs renseignements personnels; pour pouvoir être davantage elle-même grâce à l'anonymat qu'Internet peut procurer.*

b. Consultez l'annexe B, Information documentaire, pour en savoir plus.

2. Invitez les élèves à jouer à [L'imposteur](#) (un jeu dont vous êtes le héros créé avec Twine et hébergé sur Itch.io) pendant 10 minutes. Le but du jeu consiste à prendre les décisions les plus cyberfutées parmi les options proposées dans chaque scénario.

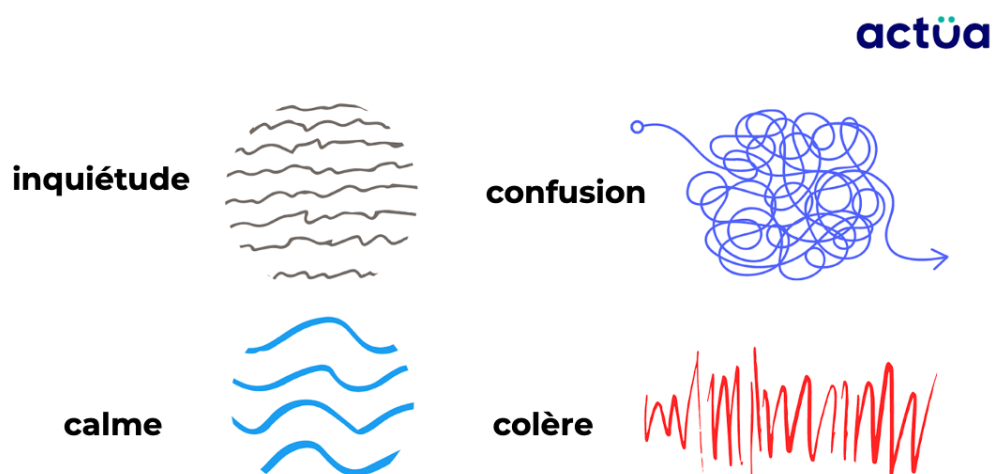
a. **Remarque** : *Les jeunes peuvent jouer individuellement ou en équipes de deux ou plus.*

3. Demandez ceci aux élèves : « **Que pouvez-vous faire si une personne en ligne vous met mal à l'aise ou que vous croyez qu'il s'agit d'un imposteur?** »

a. Réponses possibles : *On signale le compte (toutes les plateformes sociales 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, tuteur ou tuteuse, 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.*

3. Le bien-être numérique

1. Posez ces questions aux jeunes : « **Combien de temps croyez-vous passer sur votre appareil chaque jour ? Quelle proportion de ce temps est consacrée aux médias sociaux?** »
2. Présentez les mèmes fournis dans [Mèmes sur le bien-être numérique](#). « **Vous reconnaissez-vous dans certains de ces mèmes? Pourquoi?** »
3. Distribuez des feuilles de papier et des crayons de couleur aux élèves et demandez-leur de représenter leurs sentiments de manière abstraite à l'aide d'une couleur, d'une forme et d'un type de ligne (voir les exemples dans l'image ci-contre). « **Comment vous sentez-vous après avoir passé du temps en ligne?** » (À consulter votre fil d'actualité, visionner en rafale les épisodes de votre série préférée ou faire des travaux scolaires.)



4. Demandez aux élèves d'explorer (sur un ordinateur ou une tablette) les ressources en matière de bien-être et de sécurité numériques proposées par deux plateformes sociales populaires : [Meta](#) (Facebook, Instagram, WhatsApp, etc.) et [TikTok](#). Animez une discussion à partir des questions suivantes :
 - a. « **Connaissez-vous l'existence de ces ressources?** »
 - b. « **Qu'avez-vous appris de nouveau?** »
 - c. « **Qu'est-ce qui pourrait être amélioré?** »

5. Enchaînez avec ces questions : « **Quels choix sains faites-vous lorsque vous êtes en ligne? Y a-t-il d'autres choix sains que vous pourriez faire en ligne dans l'avenir? »**

a. **Remarque :** Ajoutez les éléments suivants à la liste s'ils n'ont pas été mentionnés par les élèves :

- i. Limiter le temps passé en ligne
 - 1. Prendre régulièrement des pauses d'écran
 - 2. Faire des activités de loisir sans appareil
- ii. Utilisation des médias sociaux
 - 1. Gérer les notifications
 - 2. Éviter de consulter les médias sociaux avant d'aller au lit
 - 3. Utiliser les médias sociaux à des fins précises (éviter le défilement sans but)
 - 4. Suivre des gens et des pages qu'on aime
 - 5. S'assurer que la bulle en ligne demeure sûre et positive

Réflexion et récapitulation

1. Posez les questions ci-dessous afin d'amener les jeunes à réfléchir à leur identité 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. « **Qui souhaitez-vous être en ligne? Qui souhaitez-vous être hors ligne? En quoi ces deux personnalités se ressemblent-elles? Pourquoi se distinguent-elles? »**
 - c. « **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).

À distance (en ligne)	Débranché (peu ou pas de techno)
Généralités	
• 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.	• Utilisez un tableau pour faire des remue-méninges et noter les idées et réponses des jeunes.
Introduction	

À distance (en ligne)	Débranché (peu ou pas de techno)
L'exercice peut être réalisé tel quel en ligne. Si vous laissez les élèves chercher leur nom dans Google, rappelez-leur d'examiner les résultats avec prudence avant de cliquer sur un lien (comme vous ne serez pas à leurs côtés).	Concentrez-vous sur la discussion.
1. L'empreinte numérique	
Partie 1 : La gestion de l'empreinte numérique - L'exercice peut être réalisé tel quel en ligne. Partie 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.). - Pendant la présentation des diapos, demandez aux élèves de prendre des notes (sur papier ou sur leur appareil). Partie 3 : Réflexion sur les médias sociaux	Partie 1 : La gestion de l'empreinte numérique - L'essentiel de cet exercice peut se faire tel quel, sans support technologique. Si vous ne pouvez montrer la vidéo, visionnez-la au préalable et présentez les éléments à retenir aux élèves. Partie 2 : Le surpartage - L'exercice peut être réalisé tel quel, sans support technologique. Partie 3 : Réflexion sur les médias sociaux - L'exercice peut être réalisé tel quel, sans support technologique.

À distance (en ligne)	Débranché (peu ou pas de techno)
L'exercice peut être réalisé tel quel en ligne.	
2. Qui sont les autres en ligne?	
Jouez au jeu L'impoteur (créé avec Twine) avec toute la classe et utilisez la fonction de sondage pour déterminer les décisions cyberfutées que les jeunes veulent prendre.	Rédigez des scénarios et distribuez-les aux élèves répartis en équipes. Demandez à chaque équipe de concevoir sa propre histoire à partir du scénario reçu (chaque histoire devrait comporter des décisions cyberfutées).
3. Le bien-être numérique	
L'exercice peut être réalisé tel quel en ligne.	- Imprimez les mêmes ou concentrez-vous sur la première question. - Imprimez les pages des sites web de Meta et TikTok sur le bien-être et la sécurité numériques. Demandez aux élèves de répondre aux questions en équipe.
Réflexion et récapitulation	

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.

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. L'EMPREINTE NUMÉRIQUE

- **Partie 1 : La gestion de l'empreinte numérique**
 - Créez un exemple d'empreinte numérique à montrer aux jeunes.
 - Dressez une carte en groupe plutôt que de demander aux élèves de le faire individuellement.
- **Partie 2 : Le surpartage**

- Examinez un profil avec les jeunes pour leur donner une idée des éléments à rechercher.
- Faites travailler les élèves en équipes de deux ou plus.
- Réduisez le nombre de profils à analyser.

2. QUI SONT LES AUTRES EN LIGNE?

- Jouez à [L'imposteur](#) avec toute la classe en lisant les scénarios à haute voix.

Ajouts

GÉNÉRALITÉS

- **Lien avec l'informatique :** Lancez une discussion à propos de l'intelligence artificielle.
 - 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. L'EMPREINTE NUMÉRIQUE

- **Partie 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. ([Real-Life Stories - 6 Degrees of Information](#), NetSmartz, 7:26, sous-titres en français)

- Discutez des *raisons* pour lesquelles les gens partagent trop d'information en ligne : [Your brain on likes: The science of oversharing online](#) (CBC Radio, en anglais).

3. LE BIEN-ÊTRE NUMÉRIQUE

- Invitez les jeunes à créer leurs propres mèmes (il existe de nombreux générateurs de mèmes en ligne; choisissez-en un qui est approprié pour vos élèves).

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. (13 janvier 2022). *Empreinte numérique*.

<https://cyber.gc.ca/fr/orientation/empreinte-numerique-itsap00133>

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/>

GDST. (1^{er} juillet 2016). *Live My Digital for students: Digital Footprint* [Vidéo].

<https://www.youtube.com/watch?v=OBg2YYV3Bts>

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>

Jisc. (s. d.). *Digital Wellbeing*.

<https://www.digitalcapability.jisc.ac.uk/what-is-digital-capability/digital-wellbeing/>

Meta. (s. d.). *Promouvoir la sécurité et la liberté d'expression*.

<https://about.facebook.com/fr/actions/promoting-safety-and-expression/>

Rasmussen College. (1^{er} 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>



TikTok. (s. d.). *Guide de bien-être*.

<https://www.tiktok.com/safety/fr-ca/well-being-guide/>

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, U. (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

L'EMPREINTE NUMÉRIQUE

Selon le [Centre canadien pour la cybersécurité](#) (CCC) (2022), l'empreinte numérique correspond à la trace de données qu'on crée lorsqu'on utilise Internet. Cette trace de données est issue des sites web qu'on consulte, des courriels qu'on envoie et de l'information qu'on soumet ou télécharge en ligne.

Toujours selon le CCC, l'empreinte numérique se forme de façon active et passive :

- Empreinte numérique active : Données laissées à la suite d'activités intentionnelles, telles que la publication de contenu sur les médias sociaux, le remplissage de formulaires en ligne ou l'acceptation de témoins de navigateur.
- Empreinte numérique passive : Données laissées involontairement ou sans le savoir. Ces données sont souvent recueillies par la surveillance de l'adresse IP. Les sites web et les applications peuvent installer des témoins sur les appareils sans nous en aviser, utiliser la géolocalisation ou consigner nos activités.

LE SURPARTAGE

Lorsque vous publiez du contenu dans les médias sociaux ou communiquez avec de nouvelles personnes en ligne, le surpartage 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. 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 publication 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 révélant 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 avez fourni ces renseignements 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 faux ou frauduleux sur la plateforme sociale 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.

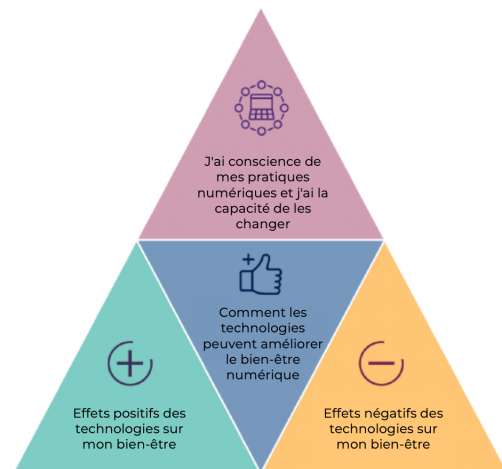
- Revoyez régulièrement vos paramètres de confidentialité.
- Gardez confidentiels vos renseignements confidentiels.
- Faites preuve de prudence dans vos interactions en ligne.

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.

LE BIEN-ÊTRE NUMÉRIQUE

Selon [Building Digital Capability](#), le terme « bien-être numérique » sert à « décrire les effets des technologies et services numériques sur la santé mentale, physique, sociale, et émotionnelle des gens (traduction libre) ».

L'image ci-contre (adapté de Jisc ,2019) montre quatre aspects du bien-être numérique d'une personne.



On peut envisager le bien-être numérique selon plusieurs points de vue. Building Digital Capability se concentre sur les points de vue individuel et sociétal ou organisationnel :

- « Point de vue individuel – contextes personnel, d'apprentissage et professionnel : La personne connaît et comprend les effets positifs et potentiellement négatifs de ses activités numériques et sait comment gérer et contrôler ces effets afin d'améliorer son bien-être.
- Point de vue sociétal ou organisationnel : Les fournisseurs de systèmes, de services et de contenus numériques sont responsables de veiller à ce que leurs produits soient bien gérés, soutenus, accessibles et équitables. Ils doivent également outiller et former les utilisateurs afin que tous puissent utiliser ces produits d'une manière qui favorise ou améliore leur bien-être (traduction libre). »

Annexe C : Autres ressources

1. L'EMPREINTE NUMÉRIQUE

Présentation PowerPoint

- [Le surpartage dans les profils de médias sociaux](#)

Vidéos

- [Live My Digital for students: Digital Footprint](#) (GDST, 4:52, sous-titres en français)
- [Teen Voices: Oversharing and Your Digital Footprint](#) (Common Sense Education, 3:34, sous-titres en français)

2. QUI SONT LES AUTRES EN LIGNE?

Site web

- [L'imposteur \(un jeu dont vous êtes le héros\)](#)

3. LE BIEN-ÊTRE NUMÉRIQUE

Présentation PowerPoint

- [*2022 : Mêmes sur le bien-être numérique](#)

Infographie

- Logos de médias sociaux (ci-dessous)

Sites web

- [Meta : Promouvoir la sécurité et la liberté d'expression](#)
- [TikTok : Guide de bien-être](#)

actüa

Exemples de médias sociaux



YouTube



Discord



Twitter



Pinterest



Snapchat



Tumblr



WhatsApp



Facebook



Tiktok



Linkedin