Ta vie privée : c'est à toi!
La valeur de la vie privée

6e et 7e année

Version du personnel enseignant

Sujets :
Vie privée et sécurité, sensibilisation des consommateurs

Durée :
Une heure à une heure et demie

Aperçu :
Dans cette leçon, les élèves apprennent que c'est avec leurs renseignements personnels que la plupart des entreprises qui proposent des applications et plateformes « gratuites » gagnent de l'argent. Ils se familiarisent avec des stratégies pratiques et des outils pour gérer leur vie privée et apprennent comment s'en servir pour limiter l'accès de différents auditoires à leurs renseignements personnels.

Dites-nous ce que vous pensez de cette leçon!

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Cette leçon a été créée par HabiloMédias pour le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario.

HabiloMédias
Le centre canadien de littératie aux médias numériques

Résultats d'apprentissage

Les élèves maîtriseront les grandes idées ou concepts clés suivants :

Les médias sont fondés sur des considérations commerciales

- Les médias comme les applications et sites Web peuvent sembler gratuits, mais nous les « payons » en leur accordant notre attention, en leur fournissant nos renseignements personnels ou les deux

Les médias numériques sont en réseau

- L'information qui circule dans un réseau peut atteindre n'importe quel élément de ce réseau

Les médias numériques sont partageables et persistants

- Toutes nos publications peuvent rester en ligne ou être partagées en permanence; elles peuvent être copiées, modifiées et utilisées de façon indésirable

Les médias numériques ont des auditoires imprévisibles

- Ce que nous publions en ligne, et les renseignements recueillis à notre sujet, peuvent être vus par un auditoire inattendu que nous ne connaissons pas nécessairement

Les élèves apprendront les connaissances essentielles suivantes dans ce domaine :

Vie privée et sécurité

- Les risques pour la vie privée comprennent les escroqueries, la gêne, le fait de blesser les gens, la cyberintimidation et les menaces pour la sécurité des biens ou des personnes
- Des mesures proactives prises pour gérer notre vie privée peuvent atténuer les risques
- Il faut faire attention aux renseignements personnels que nous partageons en ligne
- Les paramètres de confidentialité permettent de régir qui peut voir nos publications
- Les mots de passe sont un outil important pour protéger notre vie privée
- Des adultes de confiance devraient passer en revue des sites Web, applications et services au préalable, et certains devraient être interdits aux enfants
- Il est souhaitable de créer des noms d'utilisateur fondés sur des pseudonymes ainsi que des avatars pour les jeux en ligne
- Il est important de consulter des adultes de confiance avant que ne surviennent des risques pour la vie privée, et après
- Il ne faut pas cliquer sur des liens inconnus ni télécharger des fichiers provenant d'expéditeurs inconnus

Sensibilisation des consommateurs

- La plupart des entreprises qui proposent des applications « gratuites » gagnent de l'argent en vendant de la publicité, et parfois en recueillant et en vendant des renseignements personnels
- Les annonceurs paient plus si les publicités sont ciblées grâce à nos renseignements personnels
- Des plateformes utilisent également nos renseignements pour nous montrer ou recommander des contenus que nous trouvons intéressants, de sorte que nous continuons à regarder des publicités

Les élèves apprendront à :

- utiliser — gérer les risques pour la vie privée au moyen de stratégies proactives
- comprendre — déterminer les risques pour la vie privée que posent des appareils, applications et activités en ligne
- s'engager — élaborer des stratégies pour limiter les répercussions de la collecte de données sur leur expérience en ligne

Compétences en protection des données personnelles

Données personnelles

- Je comprends le concept de données personnelles, c'est-à-dire des données, qu'elles aient été rendues publiques ou non, concernant un particulier qui peut être identifié
- Je connais et je comprends le concept de pseudonymie et l'idée de camoufler mon identité
- Je peux donner des exemples de données personnelles qui permettent d'identifier une personne directement (état civil/familial, photo d'un élève de la classe, etc.) et de données techniques qui permettent de suivre les activités d'une personne et de l'identifier (témoins [« cookies »], données de géolocalisation, etc.)

Compréhension de l'environnement numérique

- Je sais ce que sont Internet et ses services (les réseaux sociaux, les applications mobiles, l'infonuagique, etc.)
- Je connais les principaux risques liés à la technologie de l'information et l'importance de la sécurité numérique, et je comprends qu'il est nécessaire d'assurer la sécurité matérielle et logique d'un environnement numérique
- Quand je m'inscris à un service, je partage uniquement les données personnelles qui sont absolument nécessaires
- Je sais qu'il existe des moyens de me protéger en ligne
- Je procède à l'évaluation de mes pratiques et développe des réflexes de résolution de problèmes et d'apprentissage — notamment en matière de sécurité — en identifiant des ressources (communautés en ligne, forums, tutoriels, etc.)
- Je connais les principaux groupes d'acteurs de l'économie numérique (p. ex., fournisseurs d'accès à Internet, fournisseurs de services, développeurs, éditeurs, etc.)
- Je comprends les systèmes utilisés pour commercialiser des produits et fournir des services gratuits (cartes de fidélité, publicités ciblées par l'enregistrement de témoins, création de comptes utilisateurs, abonnement à des bulletins, etc.) aux fins de l'établissement de profils d'utilisateur
- Je peux donner des exemples de services numériques dont le modèle économique comprend, ou ne comprend pas, la collecte de données personnelles

Gestion des données personnelles

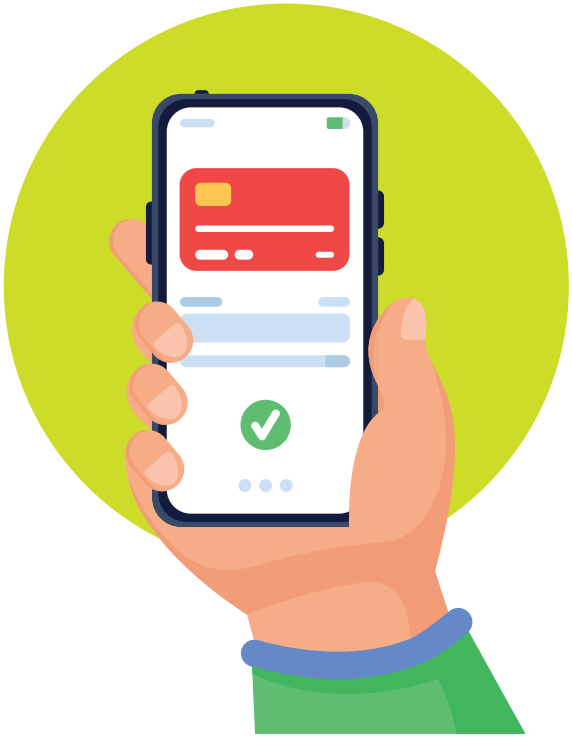
- Je sais que je peux paramétrer les applications et services en ligne que j'utilise
- Je sais que mon consentement ou celui de mes parents ou tuteurs est requis pour utiliser certains services en ligne
- Je suis des procédures courantes pour protéger mes données personnelles

Préparatifs et matériel

Préparez-vous à distribuer le livret *Ta vie privée : c'est à toi!* intégral, ou seulement les pages suivantes :

- Page 2 : Amuse-toi et apprends-en plus sur la protection de la vie privée en ligne
- Page 6 : Pourquoi s'inquiéter de la protection de la vie privée… que peut-il arriver?
- Page 9 : 11 bonnes façons de protéger la vie privée

Préparez-vous à distribuer le document *Auditoires*.



Procédure

Comment payez-vous?

Demandez d'abord aux élèves de tracer deux colonnes sur une feuille de papier. Demandez-leur ensuite de dresser deux listes d'applications qu'ils utilisent : dans la colonne de gauche, une liste des applications *payantes* (celles que l'on achète, qui comportent des frais d'abonnement ou qui permettent des achats intégrés), et dans la colonne de droite, une liste des applications *entièrement gratuites*. (S'ils ne savent pas si une application est payante ou non, dites-leur de la mettre dans la colonne des applications gratuites.)

Demandez ensuite aux élèves : Quelle est la liste la plus longue? Demandez-leur de nommer certaines applications gratuites de la colonne de droite et de les inscrire au tableau. Ces applications comprendront probablement des réseaux sociaux comme Instagram et Snapchat.

Demandez aux élèves : Si ces applications sont gratuites, comment les entreprises qui les offrent gagnent-elles de l'argent, à votre avis? Laissez les élèves suggérer quelques réponses, sans dire s'ils ont raison ou non.

Distribuez ou affichez la case « Le sais-tu? » de la page 2 et demandez aux élèves de la lire. Soulignez que quelques applications et plateformes, comme Scratch et Wikipedia, sont vraiment tout à fait gratuites, mais que dans la plupart des cas, il faut « payer » pour les applications qui semblent gratuites en leur accordant notre attention, en regardant des publicités.

Demandez maintenant : Est-ce que ces entreprises gagnent de l'argent avec vos *renseignements personnels*? Faites une pause pour passer en revue la définition de *renseignements personnels* (c'est-à-dire tout renseignement qui peut identifier une personne). Laissez les élèves discuter de cette question en vous assurant qu'ils comprennent les points suivants :

- La plupart des développeurs d'applications gratuites gagnent de l'argent en vendant des publicités.
- Les annonceurs considèrent que ces publicités sont plus utiles parce que les applications utilisent ce qu'elles savent à votre sujet (vos renseignements personnels) pour vous présenter des publicités *ciblées* susceptibles de vous intéresser.
- De nombreuses applications, y compris des réseaux sociaux comme Instagram et des sites de vidéos comme YouTube, utilisent aussi vos renseignements personnels pour déterminer quoi vous *montrer* ou vous *recommander*. Ainsi, vous restez sur ce site pendant plus longtemps et vous regardez plus de publicités.

Risques pour la vie privée

Affichez ou distribuez la page 6, « Pourquoi s'inquiéter de la protection de la vie privée… que peut-il arriver? », et demandez aux élèves de la lire.

Demandez aux élèves de représenter sur un graphique les différents risques en fonction de leur probabilité et de leur gravité éventuelle. Demandez-leur comment ils ont représenté différents risques, et discutez avec l'ensemble de la classe de la question suivante : Quels sont les risques les plus préoccupants?

Facultatif : Si vous croyez que vos élèves ont une compréhension insuffisante de ce concept, montrez-leur la vidéo *Littératie numérique 101* intitulée ***Les médias numériques ont des auditoires imprévus***.

Protéger sa vie privée

Affichez ou distribuez la page 9, « 11 bonnes façons de protéger la vie privée ». Lisez les stratégies avec les élèves et discutez avec eux de celles qui permettraient d'atténuer les risques dont vous venez de parler.

Évaluation

Distribuez le document *Auditoires*. Demandez aux élèves de choisir une application ou une plateforme qu'ils utilisent ou connaissent et d'inscrire, dans les cadres entourant l'image centrale, les auditoires possibles :

- Dans le cadre du centre, les personnes auxquelles vous voulez donner accès au contenu
- Dans le deuxième cadre, les personnes auxquelles vous ne voulez pas donner accès au contenu, mais qui pourraient le voir quand même
- Dans le troisième cadre, les personnes qui pourraient voir le contenu à votre insu, ou dans un avenir indéterminé

Invitez les élèves à ne pas penser seulement aux réseaux sociaux et aux applications de messagerie. Soulignez que tous les jeux, outils ou applications qui permettent de communiquer avec d'autres personnes, y compris les jeux vidéo dotés de fonctions de clavardage, ou les applications qui permettent de publier des contenus comme Scratch, donnent accès à ce qu'ils partagent à différents auditoires.

Ensuite, demandez aux élèves de dresser, au verso de la page, une liste des différentes stratégies (provenant de la liste de la page 9) qui empêcheraient ou limiteraient l'accès de chacun de ces auditoires à ce qu'ils publient ou partagent.

Ta vie privée : c'est à toi!

La valeur de la vie privée

6e et 7e année

Documents de l'élève

Dites-nous ce que vous pensez de cette leçon!

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Cette leçon a été créée par HabiloMédias pour le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario.

HabiloMédias
Le centre canadien de littératie aux médias numériques

Auditoires

Dans chacun des cadres ci-dessous, dresse une liste des personnes qui pourraient voir quelque chose que tu publies en ligne.

Dans le petit cadre, énumère les personnes auxquelles tu *veux* donner accès à ce contenu. Dans le cadre du milieu, indique celles qui pourraient le voir si les personnes du premier cadre le partageaient. Dans le plus grand cadre, énumère les personnes qui *pourraient* voir ce que tu publies à ton insu.

Auditoires inconnus

Auditoires indésirables

Auditoires visés

Régir les auditoires

Maintenant que tu as réfléchi aux différents auditoires qui pourraient voir ce que tu publies, indique les *stratégies de protection de la vie privée* à utiliser pour qu'il leur soit plus difficile de voir ce que tu publies ou partages. Tu peux utiliser des stratégies dans la liste des « 11 bonnes façons de protéger la vie privée » mais tu peux en ajouter d'autres aussi!

Auditoires visés : Quelles stratégies peux-tu utiliser pour que seulement *certaines* personnes que tu fréquentes en ligne puissent voir une publication?

Auditoires indésirables : Quelles stratégies peux-tu utiliser pour que tes publications soient *invisibles* aux personnes à qui tu ne veux pas les montrer?

Auditoires inconnus : Quelles stratégies peux-tu utiliser pour empêcher des gens (ou des entreprises) que tu ne connais pas de voir ce que tu regardes et fais en ligne?