PLAN DE LEÇON

LA PROTECTION DE LA VIE PRIVÉE ET SES DILEMMES

Cette leçon fait partie de *Utiliser, comprendre et mobiliser : Un cadre de littératie média numérique pour les écoles canadiennes* : https://habilomedias.ca/ressources-pedagogiques/utiliser-comprendre-et-mobiliser-un-cadre-de-litteratie-media-numerique-pour-les-ecoles-canadiennes

ANNÉES SCOLAIRE : 3e à 5e années du secondaire

A PROPOS DE L'AUTEUR : Matthew Johnson, Directeur de l'éducation, HabiloMédias

Ce plan de leçon a été réalisé grâce au soutien financier du Commissariat à la protection de la vie privée du Canada.

Aperçu

Dans cette leçon, les élèves découvrent comment les applications qu'ils utilisent sont conçues pour les inciter à partager davantage d'informations, tant avec d'autres utilisateurs qu'avec les applications elles-mêmes. Ils découvrent ensuite le concept de conception persuasive ou d'« interfaces truquées » et étudient si ces dernières sont employées pour compliquer la désinscription à la collecte de données sur des applications populaires. Enfin, la classe élabore une « galerie des interfaces truquées » pour faciliter l'identification des interfaces truquées lorsqu'ils les rencontrent.

Résultats d'apprentissage

Savoir : Les élèves apprendront…

- Analyse des médias : les types et caractéristiques des « interfaces truquées » qui incitent au partage d'informations personnelles
- Confidentialité et sécurité : les mesures techniques pour limiter la collecte de données, y compris où et comment désactiver le ciblage publicitaire et le suivi sur les applications les plus populaires.

Vocabulaire clé : données, par défaut, interface truquée

Comprendre : Les élèves comprendront que…

- Les médias sont guidés par des considérations commerciales : les informations personnelles sont précieuses pour les entreprises qui possèdent des applications et des sites Web.
- Les médias numériques ont un public inattendu : en utilisant des applications, vous donnez peut-être plus d'informations personnelles que vous ne le pensez.
- L'expérience des médias numériques est façonnée par les outils que nous utilisons : les caractéristiques et les réglages par défaut de la conception des applications et de leurs interfaces peuvent nous inciter à partager davantage d'informations que nous ne le ferions autrement.

Faire : Les élèves seront capables de…

- Identifier les façons dont les applications nous incitent à partager des informations personnelles
- Reconnaître et identifier les « interfaces truquées » qui peuvent influencer la quantité d'informations personnelles que nous partageons.
- Limiter ou désactiver la collecte de données et le suivi publicitaire sur les applications les plus populaires

Préparation et documentation

Veiller à ce que les élèves puissent accéder aux sites Web suivants :

- Google et YouTube : https://myaccount.google.com/data-and-privacy
- Facebook, WhatsApp et Instagram : https://www.facebook.com/privacy/checkup/
- TikTok : https://support.tiktok.com/fr/account-and-privacy/personalized-ads-and-data

Préparez-vous à distribuer ces documents :

- *Conçues pour le partage*
- *Interfaces truquées*
- *Audit des interfaces truquées*
- *Galerie des interfaces truquées*
- *Protéger sa vie privée sur les applications et sites Web commerciaux*

Procédure

LA PERCEPTION DE LA PROTECTION DE LA VIE PRIVÉE

Commencez par demander aux élèves quelle importance la protection de la vie privée revêt à leurs yeux. (Vous pourriez leur demander de l'évaluer sur une échelle de un à cinq, où un représente une très faible priorité et cinq, une très haute priorité.) Demandez à ceux et celles qui la jugent non importante d'expliquer pourquoi ça ne les préoccupe pas. (Peut-être seront-ils d'avis qu'ils n'ont rien à cacher, que personne ne s'intéresse à enfreindre la protection de leur vie privée ou qu'on exagère la valeur de la protection de la vie privée.) Demandez aux élèves de donner des exemples précis de risques d'atteintes ou d'atteintes réelles à la vie privée ; inscrivez-les au tableau.

À l'aide des exemples qu'auront donnés les élèves, amenez la classe à définir ce qu'est « la protection de la vie privée ». Est-ce un concept absolu (soit on la possède, soit on ne la possède pas) ou un concept relatif (la vie privée est protégée dans une mesure variable) ? Importe-t-il de protéger davantage la vie privée dans certains contextes et moins dans d'autres (en ligne par rapport à hors ligne, à la maison par rapport à l'école, etc.) ?

CONÇUES POUR LE PARTAGE

Expliquez aux élèves que de nombreuses applications sont conçues pour encourager le partage d'informations personnelles, que ce soit en publiant consciemment du contenu (comme une photo ou une vidéo) ou en interagissant avec ce contenu. Cette interaction peut aider à déduire des informations telles que vos centres d'intérêt, votre âge, votre genre, etc.

Distribuez le document *Conçues pour le partage*. Divisez les élèves en groupes ou en binômes et assignez à chaque groupe l'analyse d'une plateforme : YouTube, Instagram ou TikTok.

Demandez à chaque groupe d'analyser l'application qui lui est assignée et d'identifier comment sa conception les encourage à partager des informations personnelles. Une fois terminé, demandez aux groupes de partager leurs découvertes avec la classe et de comparer leurs réponses.

INTERFACES TRUQUÉES

Expliquez aux élèves que les caractéristiques de l'interface utilisées par les plateformes pour nous inciter à faire des choses que nous ne voulons pas faire — ou à *ne pas faire* ce que nous *voulons faire* — sont appelés *interfaces truquées*.

Distribuez le document *Interfaces truquées* et parcourez-le avec la classe. Demandez aux élèves comment chacun des exemples de la deuxième page illustre chaque catégorie :

- *Obstruction :* l'option pour accepter la collecte de données (« Accepter et continuer ») est simplifiée en une action unique immédiate, alors que personnaliser ses choix (« Gérer les paramètres ») apparaît fastidieux et dissuasif.
- *Obscurcissement :* le bouton « Accepter tout » est gros, vert et facile à trouver, alors qu'il n'y a pas de bouton « Rejeter tout » à accès facile.

- *Pression :* l'emploi d'avertissements alarmistes sur les conséquences de la désactivation de la personnalisation, ponctués de points d'exclamation pour souligner l'urgence, tout en utilisant la couleur rouge pour attirer l'attention sur le bouton d'action correspondant.

Distribuez la feuille d'exercice *Audit des interfaces truquées* et passez-la en revue avec la classe.

Demandez aux élèves de former des groupes et de choisir une application (Google/YouTube, Facebook/Instagram ou TikTok) sur laquelle au moins un membre du groupe possède un compte.

Si aucun élève d'un groupe ne dispose d'un compte sur l'une de ces trois applications, demandez-leur d'utiliser ce compte Google :

ExampleID1996@google.com Mot de passe : **i:N9HuCVnHTjY6**

Demandez maintenant aux élèves de suivre les instructions de la feuille d'exercice.

Après une dizaine de minutes de travail, vérifiez qu'ils ont pu trouver comment changer leurs paramètres de collecte de données ou désactiver le ciblage publicitaire. S'ils n'y sont pas parvenus, donnez-leur le lien approprié :

- Google et YouTube : https://myaccount.google.com/data-and-privacy
- Facebook, WhatsApp et Instagram : https://www.facebook.com/privacy/checkup/
- TikTok : https://support.tiktok.com/fr/account-and-privacy/personalized-ads-and-data

GALERIE DES INTERFACES TRUQUÉES

Distribuez la feuille de travail *Galerie des interfaces truquées* et parcourez-la avec la classe. Demandez à chaque élève (ou, si vous préférez, à chaque binôme ou groupe) de choisir **une** interface truquée qu'il a identifié dans les activités *Conçues pour le partage* ou *Audit des interfaces truquées* et de créer un « avis de recherche » qui aidera d'autres personnes à la reconnaître.

Lorsque les élèves ont terminé leurs affiches, accrochez-les dans la salle. Distribuez des notes adhésives ou des trombones aux élèves, puis demandez-leur de de faire le tour des affiches et de mettre une note

adhésive ou un trombone sur chaque affiche représentant une interface qu'ils ont déjà rencontrée sur un site Web ou une application.

Lorsque les élèves ont fini de faire le tour des affiches, voyez celles qui ont le plus de notes adhésives ou de trombones. Demandez aux élèves pourquoi ils pensent que ces interfaces truquées sont les plus courantes dans les applications destinées aux enfants/adolescents et ce qu'ils pourraient faire pour les éviter ou les reconnaître.

RÉFLEXION

Distribuez le document *Protéger sa vie privée sur les applications et sites Web commerciaux*. En guise de réflexion ou de billet de sortie, demandez aux élèves de le lire et de réfléchir aux questions suivantes :

- Mettez-vous déjà en pratique certaines de ces recommandations?
- Y a-t-il des conseils donnés dans ce document que vous souhaiteriez commencer à mettre en pratique?
- Y a-t-il des points que vous aimeriez aborder avec vos parents afin de les mettre en pratique?

DOCUMENT D'ACCOMPAGNEMENT

LA PROTECTION DE LA VIE PRIVÉE ET SES DILEMMES

Conçues pour le partage

Choisissez YouTube, Instagram ou Tiktok et utilisez ce document pour identifier les fonctionnalités de ces applications et la manière dont elles vous incitent à partager davantage d'informations personnelles. Nous avons donné des exemples de Snapchat pour illustrer les différents types de fonctionnalités auxquelles vous devez penser. Votre tâche consiste à trouver des exemples similaires sur Instagram.

Dans le tableau au verso, dressez la liste des fonctionnalités de l'application dans la colonne de gauche. Les fonctionnalités sont les actions que vous pouvez faire avec l'application. Certaines décrivent une action générale (comme partager une photo) tandis que d'autres sont plus spécifiques à l'application (comme l'envoi d'une photo éphémère avec Snapchat).

Assurez-vous de prendre en compte :

- La création et le remplissage de votre profil
- Le partage de publications, de photos ou de vidéos
- La gestion de la visibilité de vos contenus
- Les interactions avec les contenus d'autres personnes (réponses, partages, etc.)
- La manière dont les autres réagissent à vos publications (J'aime, partages, etc.)
- Les réactions de l'application à vos publications ou à celles de vos amis (les flammes sur Snapchat, par exemple)

Pour chaque fonctionnalité, précisez au centre si elle est par défaut (si elle se produit automatiquement ou sauf si vous indiquez le contraire), si elle est facile ou difficile à utiliser (en général, une action qui nécessite un ou deux tapotements ou clics est facile; celle qui en nécessite trois ou plus est difficile).

Par exemple, sur Snapchat, les amis voient votre Story *par défaut*. Il est facile d'envoyer un Snap et difficile de modifier vos paramètres de confidentialité par défaut.

Dans la colonne de droite, notez comment ces fonctionnalités — et le fait qu'elles soient par défaut, faciles ou difficiles à utiliser — influencent la quantité d'informations personnelles que vous partagez. Ne pensez pas seulement à vos propres informations, mais aussi à celles de vos amis!

QUELLE APPLICATION ANALYSEZ-VOUS?

FONCTIONNALITÉ	PAR DÉFAUT, FACILE OU DIFFICILE?	IMPACT SUR LA VIE PRIVÉE

DOCUMENT D'ACCOMPAGNEMENT

LA PROTECTION DE LA VIE PRIVÉE ET SES DILEMMES

Interfaces truquées

Les « interfaces truquées » sont des techniques utilisées par les applications pour nous inciter à faire des choses que nous ne voudrions peut-être pas faire. Elles peuvent également nous *dissuader* de faire ce que nous souhaitons réellement faire. Dans cet exercice, nous examinerons comment ces interfaces nous incitent à **divulguer davantage d'informations personnelles** et à négliger les **mesures de contrôle de notre vie privée**.

Il existe trois grands types d'interfaces truquées en matière de protection de la vie privée :

Obstruction : Rendre plus difficile les actions qui protègent la vie privée.

- Faire de la collecte de données un choix *par défaut* (vous devez donc faire une action pour que vos informations personnelles ne soient *pas* collectées).
- Ajouter des étapes supplémentaires pour vous faire confirmer que vous ne voulez pas que vos données soient collectées.
- Faciliter l'acceptation plutôt que le rejet de la collecte de données.

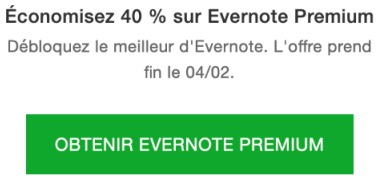
Obscurcissement : Rendre plus difficile la localisation des outils qui nous permettent de protéger notre vie privée.

- Rendre les options de confidentialité difficiles à trouver.
- Rendre les boutons ou autres fonctionnalités qui permettent la collecte de données plus évidents ou attrayants.
- Ne pas être clair sur les données que vous **devez** fournir et celles qui sont optionnelles.
- Rendre vos choix confus
- Suggérer que certains outils ou options protègent davantage votre confidentialité qu'ils ne le font réellement (comme le mode « Incognito »)

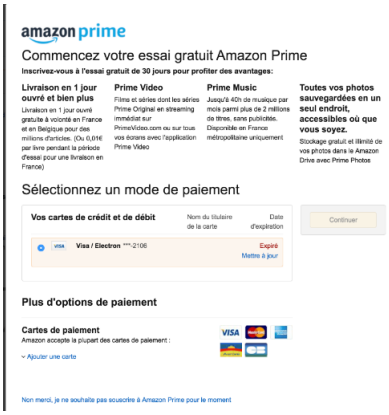
Pression : Vous faire croire qu'il est bon d'accepter la collecte de données ou vous faire sentir coupable de protéger votre vie privée.

- Rendre l'application plus difficile à utiliser si vous ne partagez pas vos informations personnelles.
- Vous faire peur en vous expliquant ce que vous perdrez ou n'obtiendrez pas si vous ne communiquez pas vos informations personnelles.
- Ne pas vous permettre de refuser de manière catégorique.

OBSTRUCTION :



OBSCURCISSEMENT :



PRESSION :

DOCUMENT D'ACCOMPAGNEMENT

LA PROTECTION DE LA VIE PRIVÉE ET SES DILEMMES

Audit des interfaces truquées

Dans quelle mesure est-il difficile de désactiver la collecte de données et le ciblage publicitaire sur les différentes applications?

Répondez aux questions suivantes sur une feuille à part :

1. Commencez par vous connecter à Google, Instagram ou TikTok. Notez l'application choisie :
2. Essayez maintenant de trouver la page permettant de modifier vos paramètres de collecte de données ou de désactiver le suivi et le ciblage publicitaire.
    - Avez-vous pu la trouver?
    - Si oui, a-t-elle été difficile à trouver?
    - Combien de clics ou de tapotements ont été nécessaires?
3. Essayez maintenant de désactiver la collecte de données et le ciblage publicitaire.
    - Dans quelle mesure la tâche est-elle facile ou difficile?
    - Êtes-vous certain de comprendre à quoi vous avez consenti?
4. L'application a-t-elle utilisé des *interfaces truquées…*
    - Lorsque vous avez essayé de trouver la page?
    - Lorsque vous avez essayé de désactiver la collecte de données ou le ciblage publicitaire?

Décrivez les exemples que vous avez trouvés pour chaque type d'interface truquée :

- *Obstruction*
- *Obscurcissement*
- *Pression*

DOCUMENT D'ACCOMPAGNEMENT

LA PROTECTION DE LA VIE PRIVÉE ET SES DILEMMES

Galerie des interfaces truquées

Choisissez l'un des trois types d'interfaces truquées :

Obstruction (rendre plus difficiles les actions qui limitent la divulgation de données privées);

Obscurcissement (rendre plus difficile la recherche des outils permettant de protéger notre vie privée); ou

Pression (vous donner l'impression qu'il vaut mieux accepter la collecte de données ou vous faire sentir coupable de vouloir protéger votre vie privée).

(Relisez le document sur les *interfaces truquées* pour vous remémorer la définition et les exemples de chacune).

Vous allez maintenant créer un avis de recherche qui aidera les gens à reconnaître cette interface truquée lorsqu'ils la verront. L'affiche doit comporter les éléments suivants :

- Le nom de l'interface truquée
- Un graphique ou un dessin pour l'illustrer
- La raison pour laquelle elle est recherché (pourquoi est-elle dangereuse?)
- Ses caractéristiques distinctives (comment la reconnaîtrez-vous?)
- Ce que vous devriez faire lorsque vous la voyez

Votre produit final doit être imprimable afin que nous puissions exposer les affiches dans la salle de classe.

DOCUMENT D'ACCOMPAGNEMENT

LA PROTECTION DE LA VIE PRIVÉE ET SES DILEMMES

Protéger sa vie privée sur les applications et sites Web commerciaux

La majorité des applications et sites Web préférés des enfants génèrent des revenus grâce à la *publicité ciblée*, qui utilise leurs données personnelles pour sélectionner les annonces qui leur seront présentées. En outre, beaucoup vendent ces données à des courtiers de données, qui collectent des données provenant de nombreuses sources pour établir des profils détaillés des utilisateurs. Souvent, ces informations sont également partagées avec d'autres applications de la même entreprise comme Google, Instagram ou Facebook.

Selon William Budington de l'Electronic Frontier Foundation, « vous pouvez prendre des mesures pour protéger votre vie privée à 85, 90, 95 % qui n'ajouteront pas beaucoup de contraintes à votre vie. » En voici quelques-unes :

- Installez des plugiciels de protection de la vie privée comme **Privacy Badger** sur les ordinateurs portables et de bureau et des applications comme **DuckDuckGo** ou **Do Not Track Kids** sur les appareils mobiles.
- Examinez les données que les différentes applications collectent sur les appareils mobiles.
- Consultez et personnalisez vos paramètres de confidentialité. Par exemple, voici comment désactiver le suivi et les publicités ciblées sur :
    - Google et YouTube : https://myaccount.google.com/data-and-privacy
    - Facebook, WhatsApp et Instagram : https://www.facebook.com/privacy/checkup/
    - TikTok : https://support.tiktok.com/fr/account-and-privacy/personalized-ads-and-data
- Ne vous inscrivez pas sur des applications ou des sites Web en utilisant vos identifiants de médias sociaux. Vous pouvez également créer des adresses courriel sécurisées et jetables à l'aide de Protonmail ou Sharklasers si vous souhaitez créer un compte sans divulguer votre adresse courriel habituelle.
- Allez dans les paramètres de votre appareil et désactivez l'accès des applications à l'appareil photo, au microphone et à la localisation.
- Si vous utilisez des appareils iOS comme des iPhone ou des iPad, veillez à refuser la collecte de données lors de l'installation de nouvelles applications. Si vous utilisez des appareils Android, installez l'application DuckDuckGo et activez la protection contre le suivi des applications.
- N'acceptez que le niveau minimum requis de collecte de données sur les sites Web — tout d'abord, en ne cliquant jamais sur « Accepter tout », puis en recherchant des phrases telles que « Rejeter tout » ou « Seulement le nécessaire ».

