PLAN DE LEÇON

MARKETING EN LIGNE DESTINÉ AUX JEUNES : PROTÉGEZ VOTRE VIE PRIVÉE

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 : 6e à 9e année ; 6e année à 3e secondaire

A PROPOS DE L'AUTEUR : HabiloMédias

Aperçu

Cette leçon permet aux élèves de se familiariser avec les différentes techniques utilisées par les applications et les sites Web commerciaux pour recueillir des renseignements personnels sur les enfants. La leçon permet également de comprendre les enjeux relatifs aux enfants et à la protection de la vie privée sur Internet. Les élèves commencent par se demander s'ils seraient à l'aise que des personnes puissent connaître diverses informations à leur sujet, puis visionnent une vidéo expliquant le fonctionnement de la publicité ciblée et en discutent. Ils explorent ensuite le concept de publicité ciblée par le biais d'un exercice en classe dans lequel le Prince charmant essaie de cibler Cendrillon avec une publicité pour des pantoufles de verre, puis analysent comment leurs propres informations personnelles pourraient être utilisées pour les cibler avec des publicités. Dans la deuxième partie de la leçon, les élèves sont initiés aux politiques de protection de la vie privée et à la manière dont elles sont évaluées par le site Web *Terms of Service, Didn't Read*. Ils lisent et analysent l'évaluation que fait le site d'une application populaire, puis apprennent à limiter la collecte de données. Dans le cadre d'une activité complémentaire, les élèves découvrent le concept d'« interfaces truquées » et imaginent comment la méchante Reine pourrait les utiliser pour pousser Blanche-Neige à accepter des cookies « empoisonnés ».

Objectifs visés

Savoir : les élèves apprendront…

- Confidentialité et sécurité :
  - Comment les informations personnelles sont utilisées pour le ciblage publicitaire.
  - Les répercussions possibles de la collecte de données.
  - Ce que sont les politiques de protection de la vie privée.
- Les moyens techniques pour restreindre la collecte de données, y compris où et comment désactiver le ciblage et le suivi publicitaire sur les applications populaires.

- Sensibilisation des consommateurs :
  - Comment les applications et autres plateformes en ligne gagnent de l'argent.
  - Comment et pourquoi les plateformes en ligne utilisent la publicité ciblée.

Lexique : données, informations personnelles, publicité ciblée, politique de confidentialité, 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.

Idée reçue à clarifier : l'existence d'une politique de confidentialité ne signifie pas qu'un service ne collecte pas de données, elle détaille simplement comment le service peut collecter et utiliser vos données.

Faire : Les élèves seront capables de…

- Identifier comment les annonceurs peuvent les cibler en utilisant leurs informations personnelles.
- Évaluer une politique de confidentialité.
- Prendre des mesures pour limiter la collecte de données lors de l'utilisation d'applications et de sites Web.

Préparation et documents

Passez en revue le document d'information à l'intention de l'enseignant *Les applications pour enfants les plus populaires*

Préparez la distribution des documents suivants :

- *Que saurait-on de vous si l'on savait…*

- *À la recherche de Cendrillon*
- *La cible, c'est vous*
- *Conditions d'utilisation et politiques de confidentialité*
- *Audit sur la protection de la vie privée*
- *Protéger sa vie privée sur les applications et sites Web commerciaux*

Si vous réalisez l'activité complémentaire, distribuez le document Interfaces truquées

Procedure

PREMIÈRE PARTIE : COMPRENDRE LA PUBLICITÉ CIBLÉE

Commencez par distribuer le document *Que saurait-on de vous si l'on savait…* et demandez aux élèves d'imaginer ce que les gens sauraient d'eux s'ils connaissaient… :

- Leur adresse.
- Les vidéos qu'ils ont regardées en ligne.
- Leurs activités sur les médias sociaux (ce qu'ils ont publié, regardé, commenté, aimé, etc.).
- Leurs achats en ligne.
- Leurs achats en magasin.
- Leurs recherches sur internet.

Demandez aux élèves d'écrire au moins deux éléments pour chaque catégorie, en leur précisant qu'ils ne seront pas obligés de partager leurs réponses. (Cette activité peut aussi être donnée en tant que devoir à faire à la maison la veille).

Une fois que les élèves ont terminé, demandez-leur :

- Seriez-vous à l'aise avec le fait que des gens sachent ces informations sur vous?
- Certaines informations sont-elles plus privées ou plus sensibles que d'autres? (Les élèves n'ont pas besoin de donner des exemples précis, ils peuvent simplement indiquer quelles catégories leur semblent plus ou moins sensibles, par exemple, leurs achats par rapport à leurs recherches en ligne.)

- Y a-t-il des informations que vous seriez prêts à partager avec certaines personnes (comme des amis proches ou de la famille)?
- Y a-t-il des informations que vous ne voudriez que personne ne sache?

FONCTIONNEMENT DE LA PUBLICITÉ CIBLÉE

Si aucun élève n'a encore soulevé ce point, faites-leur remarquer que certaines personnes sont déjà au courant de tout ce qu'ils ont listé : il s'agit des entreprises qui gèrent les applications numériques, les sites Web et les appareils. Tous ces éléments sont des exemples d'*informations personnelles* ou de *données personnelles* collectées par les entreprises.

Demandez aux élèves s'ils savent pourquoi les entreprises collectent autant d'informations personnelles.

Après avoir laissé les élèves en discuter pendant quelques minutes, montrez-leur la vidéo *Fonctionnement de la publicité ciblée*.

Puis, posez les questions de consolidation suivantes :

Comment les applications telles que les médias sociaux (Instagram, Snapchat, etc.) ou les plateformes de vidéos (YouTube, etc.) génèrent-ils des revenus?

> En vous présentant des publicités.

En quoi le fait d'en connaître davantage sur vous peut-il les aider à gagner de l'argent?

> Expliquez que, en plus de vous cibler avec des publicités, les applications utilisent vos données pour vous proposer du contenu qui vous incitera à passer plus de temps à les utiliser.

La publicité ciblée est-elle infaillible?

Non, elle ne l'est pas toujours, car les données collectées peuvent être erronées (par exemple, si vous partagez un appareil ou un compte) ou les suppositions basées sur ces données peuvent s'avérer incorrectes.

Quels sont les risques ou les inconvénients des publicités ciblées?

- Vous pourriez être ciblé sur la base de caractéristiques qui ne devraient pas être utilisées.

- Si le profil établi sur vous est inexact, vous pourriez passer à côté de publicités ou de contenus qui auraient pu vous intéresser.
- Les personnes traversant des périodes vulnérables, comme juste après un diagnostic de maladie grave, pourraient être la cible de publicités frauduleuses.
- Les données collectées à votre sujet pourraient être utilisées à d'autres fins pendant des années.

À LA RECHERCHE DE CENDRILLON

Distribuez maintenant le document *À la recherche de Cendrillon*.

Demandez aux élèves s'ils connaissent l'histoire de Cendrillon et racontez (ou faites raconter par un élève) l'essentiel :

- Cendrillon vivait avec une méchante belle-mère et deux méchantes demi-sœurs.
- Sa marraine la fée lui a donné par magie une robe, un carrosse et des pantoufles de verre pour qu'elle puisse se rendre au bal royal.
- Cendrillon a rencontré le Prince charmant au bal mais a dû s'enfuir avant minuit.
- Elle a laissé une de ses pantoufles de verre derrière elle.
- Le Prince charmant s'est rendu dans toutes les maisons à la recherche de celle dont le pied rentrerait dans la chaussure, et a fini par trouver Cendrillon.

Demandez aux élèves d'imaginer que, plutôt que de passer de maison en maison, le Prince charmant utilise maintenant la publicité ciblée pour trouver Cendrillon avec une publicité pour des pantoufles de verre. Comment procéderait-il?

Demandez-leur de réfléchir à ce qu'il sait déjà sur sa « cible », Cendrillon :

- Son genre apparent
- Son âge approximatif
- Sa localisation générale
- Sa pointure

Quelles informations *inexactes* pourrait-il avoir sur elle?

Questions incitatives :

Pourquoi pourrait-il se faire une idée erronée de ses revenus? (À cause de la robe et du carrosse que sa marraine la fée lui a offerts)

Pensez-vous qu'elle ait son propre téléphone? Quelles pourraient être les implications si elle partageait un téléphone avec ses belles-sœurs ou sa belle-mère?

Que pourrait-il déduire sur elle à partir de :

- Son historique de recherche?
- Son historique de visionnage sur *YouTube* ou *Netflix*?
    - Regarde-t-elle des tutoriels sur le nettoyage? Des films romantiques avec des princes?
- Son activité (visionnage, publications, commentaires, mentions « J'aime », partages) sur les médias sociaux comme *Instagram*, *Snapchat* ou *TikTok*?
    - A-t-elle évoqué le bal sur les médias sociaux? Mentionné sa marraine la fée? Plainte de sa belle-mère ou de ses demi-sœurs? Essaie-t-elle de remplacer sa pantoufle manquante?
    - A-t-elle « aimé » l'une des photos du bal publiées par le Prince?
    - Ses achats en ligne
    - Si elle a déjà acheté des chaussures en ligne, il pourrait la retrouver grâce à sa pointure!

LA CIBLE, C'EST VOUS

Maintenant, distribuez le document *La cible, c'est vous* et demandez aux élèves de le remplir individuellement. Demandez à chaque élève de réfléchir à ces questions :

- Quelles informations les annonceurs en ligne pourraient-ils savoir ou supposer à votre sujet?
- Sur quelles données se baseraient-ils pour faire ces suppositions?
- Que pourraient-ils croire savoir sur vous qui est faux? Pourquoi?
- Quelles sont les publicités qu'ils pourraient vous montrer en fonction de ce qu'ils savent ou supposent à votre sujet?
- Quels pourraient être les « effets secondaires » du partage des informations qu'ils détiennent sur vous?

Demandez à chaque élève d'exprimer ce que cet exercice leur a fait ressentir vis-à-vis du ciblage publicitaire et de la collecte de données. (Ils n'ont pas à partager leurs réponses spécifiques.) Utilisez ces réactions pour évaluer leur compréhension des concepts clés et des connaissances fondamentales abordées jusqu'à présent.

Si vous le souhaitez, vous pouvez leur demander d'écrire un essai à la suite de cette activité, avec la consigne suivante : Avant, je pensais que la vie privée… Maintenant, je pense que…

DEUXIÈME PARTIE : PROTÉGER VOTRE VIE PRIVÉE

ÉVALUER DES POLITIQUES DE CONFIDENTIALITÉ

Demandez maintenant aux élèves s'ils savent ce qu'est la **politique de confidentialité** d'une application et à quoi elle sert. Il faut clarifier une idée reçue : contrairement à ce que beaucoup pensent, le fait qu'une application dispose d'une politique de confidentialité ne signifie pas qu'elle ne collectera *aucune* information vous concernant. La politique de confidentialité indique :

- Les informations recueillies;
- Les utilisations autorisées de ces données;
- Les tiers avec lesquels elles peuvent être partagées; et
- La durée de conservation de ces données, entre autres.

Posez maintenant la question : combien de temps pensez-vous qu'il faudrait pour lire intégralement les conditions d'utilisation et la politique de confidentialité de :

- Instagram? (Environ neuf heures et demie).
- YouTube? (Treize heures et quarante-cinq minutes).
- Amazon? (Quatorze heures).
- TikTok? (Trente et une heures et demie).

(Estimations titrées de : https://coeursurparis.com/combien-de-temps-faut-il-pour-lire-les-conditions-dutilisation-de-chaque-application-infographic/)

Distribuez le document *Conditions d'utilisation et politiques de confidentialité* et parcourez-le avec la classe. Distribuez ensuite la feuille d'activité *Audit de la protection de la vie privée*.

Si possible, utilisez un vidéoprojecteur ou un tableau blanc numérique pour montrer aux élèves le site Web *Terms of Service, Didn't Read* (tosdr.org). Recherchez les conditions d'utilisation de Google et montrez aux élèves les conditions d'utilisation marquées en rouge, jaune, vert et gris.

Ensuite, divisez la classe en binômes ou en petits groupes. Attribuez à chaque binôme ou groupe une des applications mentionnées dans le document *Les applications pour enfants les plus populaires* et demandez-leur ensuite d'accéder au site Web *Terms of Service, Didn't Read* pour réaliser l'audit de protection de la vie privée.

Lorsque les élèves ont terminé, demandez-leur de partager leurs découvertes avec le reste de la classe :

- Quelle classe leur application a-t-elle obtenue?
- Ont-ils été surpris? Pourquoi?
- Pensent-ils que la classe obtenue est juste? Pourquoi?
- Si plusieurs groupes ont évalué la même application :
    - Ont-ils identifié les mêmes conditions d'utilisation en rouge et en jaune comme étant les plus préoccupantes?
    - Ont-ils identifié les mêmes conditions d'utilisation en vert comme étant les plus rassurantes?
    - S'il y a des différences entre les évaluations des équipes, demandez-leur d'expliquer leur raisonnement.
- Le fait de connaître la classe de l'application les rend-il plus ou moins enclins à l'utiliser? Pourquoi?

PROTÉGER VOTRE VIE PRIVÉE

Si aucun élève n'a soulevé ce point lors de la dernière discussion, demandez-leur :

- Vous arrive-t-il de vous sentir obligé d'utiliser une application ou un service, même si vous n'êtes pas à l'aise avec son impact sur votre vie privée, simplement parce que vos amis l'utilisent?
- Parce que vos parents l'utilisent pour vous contacter?
- Êtes-vous parfois obligé d'utiliser l'un de ces services pour participer à l'école ou à une activité?

PROTÉGER VOTRE VIE PRIVÉE

Dites aux élèves que l'utilisation d'une application ou d'un autre service en ligne n'est pas forcément un choix binaire : il existe des moyens de limiter la quantité d'informations collectées et leur utilisation.

Distribuez le document *Protéger sa vie privée sur les applications et les sites Web commerciaux*.

Une fois que vous l'avez parcouru avec la classe, demandez :

- 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?

Demandez-leur de se remémorer l'audit sur la protection de la vie privée qu'ils ont effectué précédemment, et en particulier les éléments de la politique de confidentialité de l'application qui les ont mis mal à l'aise. Demandez-leur maintenant de choisir **trois** des conseils donnés dans le document *Protéger sa vie privée sur les applications et les sites Web commerciaux* qui les rendraient plus à l'aise dans l'utilisation de l'application, et de rédiger une courte explication (2 à 3 phrases chacun) sur la manière dont ce conseil particulier les aiderait à protéger leur vie privée.

ACTIVITÉ COMPLÉMENTAIRE : LES INTERFACES TRUQUÉES

Expliquez aux élèves que même si nous souhaitons protéger notre vie privée, les applications ne nous facilitent pas toujours la tâche. Les moyens par lesquels elles nous incitent 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.

Demandez aux élèves s'ils connaissent l'histoire de Blanche-Neige. Assurez-vous qu'ils se souviennent de la partie où la Reine Maléfique pousse Blanche-Neige à manger une pomme empoisonnée, et dites-leur qu'ils vont imaginer qu'elle utilise des interfaces truquées pour pousser Blanche-Neige à accepter des « cookies » empoisonnés.

Demandez aux élèves de trouver un exemple de chaque type d'interface truquée qu'elle pourrait utiliser. Ils peuvent dessiner une boîte de consentement des cookies sur l'écran du téléphone intelligent du document, utiliser une feuille de papier vierge, ou la dessiner numériquement.

Un bon citoyen d'Internet prend certaines mesures lorsqu'il remarque un contenu douteux comme des pratiques de marketing en ligne intrusives. Demandez aux élèves d'utiliser leurs découvertes de l'activité 1 pour écrire une lettre à un site Web destiné aux enfants dont le contenu porte atteinte à la vie privée des enfants. Si les élèves n'ont pas trouvé de sites Web qui portent atteinte à la vie privée des enfants, demandez-leur d'écrire une lettre recommandant des changements à l'un des trois documents qu'ils ont lus sur la vie privée des enfants en ligne.

DOCUMENT D'ACCOMPAGNEMENT

MARKETING EN LIGNE DESTINÉ AUX JEUNES : PROTÉGEZ VOTRE VIE PRIVÉE

Que saurait-on de vous si l'on savait...

Citez au moins deux choses que l'on pourrait savoir (ou penser savoir) sur vous en fonction de chacun de ces éléments :

Les vidéos que vous regardez en ligne

Vos activités sur les médias sociaux (ce que vous avez publié, regardé, commenté, aimé, etc.)

Vos achats en ligne

Vos achats en magasin

Vos recherches sur internet

DOCUMENT D'ACCOMPAGNEMENT

MARKETING EN LIGNE DESTINÉ AUX JEUNES : PROTÉGEZ VOTRE VIE PRIVÉE

À la recherche de Cendrillon

Pour cet exercice, nous allons imaginer que le Prince charmant utilise des publicités ciblées pour retrouver Cendrillon qui s'est enfuie du bal.

Que sait-il déjà sur sa « cible »?

Que peut-il *croire* savoir sur elle (mais qui est faux)?

Que pourrait-il apprendre sur elle?

- Son historique de recherche?

- Son historique de visionnage sur *YouTube* ou *Netflix*?

- Son activité (visionnage, publications, commentaires, mentions « J'aime », partages) sur les médias sociaux comme *Instagram*, *Snapchat* ou *TikTok*

- Ses achats en ligne?

DOCUMENT D'ACCOMPAGNEMENT

MARKETING EN LIGNE DESTINÉ AUX JEUNES : PROTÉGEZ VOTRE VIE PRIVÉE

La cible, c'est vous

Vous allez maintenant imaginer comment les applications, les sites Web et les courtiers en données vous ciblent.

Réfléchissez à ce que vous avez appris sur la publicité ciblée et donnez au **moins deux réponses** à chacune de ces questions :

- Quelles informations les annonceurs en ligne pourraient-ils savoir ou supposer à votre sujet?

- Sur quelles données se baseraient-ils pour faire ces suppositions?

- Que pourraient-ils croire savoir sur vous qui est faux? Pourquoi?

- Quelles sont les publicités qu'ils pourraient vous montrer en fonction de ce qu'ils savent ou supposent à votre sujet?

- Quels pourraient être les « effets secondaires » du partage des informations qu'ils détiennent sur vous?

DOCUMENT D'ACCOMPAGNEMENT

MARKETING EN LIGNE DESTINÉ AUX JEUNES : PROTÉGEZ VOTRE VIE PRIVÉE

Conditions d'utilisation et politique de confidentialité

Les politiques de confidentialité décrivent les conditions de confidentialité d'un site particulier. Cependant, beaucoup de ces politiques sont vagues, trompeuses ou inexistantes, en plus d'être très longues : c'est pourquoi seulement la moitié des enfants canadiens ont déjà lu une ou ont demandé à quelqu'un de le faire avec eux.

Heureusement, il n'est pas nécessaire de lire toute la politique pour comprendre comment elle affectera votre vie privée. Lorsque vous lisez une politique de confidentialité, recherchez des titres tels que :

- « Informations personnelles que nous collectons » ou « comment collectons-nous vos données personnelles? ».
- « Géolocalisation » ou « géociblage » : si une application souhaite accéder à votre emplacement sans raison apparente, vous devrez peut-être désactiver le GPS sur votre appareil.
- « Comment utilisons-nous vos informations personnelles? » : recherchez des termes vagues tels que « activités commerciales » ou « objectifs commerciaux ».
- « Personnaliser », « améliorer », « améliorer vos services » ou « publicité basée sur les intérêts » : si la politique contient ce type de formulation, vérifiez si vous pouvez désactiver le tri algorithmique (par exemple en passant du flux « Pour toi » au flux « Abonnements ») et la publicité ciblée.
- « Vos droits » ou « vos choix » : cela décrira généralement les options qui s'offrent à vous en vertu de la législation en vigueur dans votre pays.

Le site Web **Terms of Service, Didn't Read** (tosdr.org) classe de **A** à **E** les conditions d'utilisation et les politiques de confidentialité de différentes applications et sites Web :

A : « ce sont les meilleures conditions d'utilisation : elles vous traitent de façon juste, respectent vos droits et n'abuseront pas de vos données »

B : « les conditions d'utilisation sont justes envers les utilisateurs mais pourraient être améliorées »

C : « les conditions d'utilisation sont assez bonnes, mais certains problèmes requièrent votre considération »

D : « les conditions d'utilisation sont très injustes ou il y a des problèmes importants qui exigent votre attention »

E : « les conditions d'utilisation soulèvent de très sérieuses préoccupations »

Ces évaluations sont basées sur l'opinion des bénévoles du site, mais ils donnent des raisons spécifiques pour lesquelles chaque classe est attribuée :

- **Rouge (bloqueur) :** conditions d'utilisation qui sont sérieusement injustes pour l'utilisateur
- **Jaune (mauvais) :** conditions d'utilisation qui soulèvent des préoccupations
- **Vert (bon) :** conditions d'utilisation qui protègent ou renforcent les droits de l'utilisateur
- **Gris (neutre) :** conditions d'utilisation ayant un impact neutre sur l'entreprise et l'utilisateur

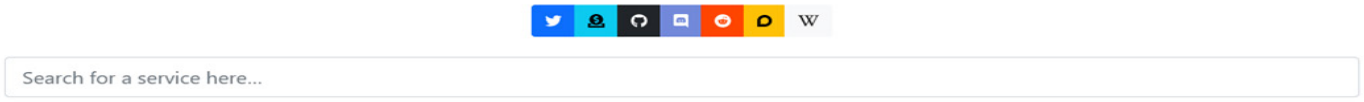
DOCUMENT D'ACCOMPAGNEMENT

MARKETING EN LIGNE DESTINÉ AUX JEUNES : PROTÉGEZ VOTRE VIE PRIVÉE

Audit de la protection de la vie privée

1. Dressez la liste des applications à auditer :

2. Allez sur la page d'accueil de *Terms of Service, Didn't Read* (tosdr.org) et recherchez l'application. **Si elle n'y figure pas, choisissez-en une autre.** La barre de recherche se trouve en haut de la page, juste au-dessus des classes présentées :



Inscrivez la classe de l'application (de A à E) ci-dessous :

3. S'il y a des conditions d'utilisation en **rouge**, citez les **deux** qui, selon vous, ont le plus **mauvais** impact sur votre vie privée.

4. S'il y a des conditions d'utilisation en **jaune**, citez les **deux** qui, selon vous, ont le plus **mauvais** impact sur votre vie privée.

5. S'il y a des conditions d'utilisation en **vert**, citez les **deux** qui, selon vous, **protègent** le mieux votre vie privée.

Répondez aux questions suivantes sur une feuille séparée :

6. La classe obtenue par l'application vous a-t-elle surpris? Pourquoi?

7. Pensez-vous que la classe obtenue est juste? Pourquoi?

8. Le fait de connaître la classe de l'application vous rend-il plus ou moins enclin à l'utiliser? Pourquoi?

DOCUMENT D'ACCOMPAGNEMENT

MARKETING EN LIGNE DESTINÉ AUX JEUNES : PROTÉGEZ VOTRE VIE PRIVÉE

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 ».

PLAN DE CONFIDENTIALITÉ :

Repensez à l'audit sur la protection de la vie privée que vous avez réalisé précédemment.

Choisissez **trois** des conseils ci-dessus qui vous permettraient de vous sentir plus à l'aise dans l'utilisation de cette application.

Rédigez 2 à 3 phrases pour **chaque** conseil en expliquant pourquoi il protège votre vie privée lorsque vous utilisez l'application en question.

DOCUMENT D'ACCOMPAGNEMENT

MARKETING EN LIGNE DESTINÉ AUX JEUNES : PROTÉGEZ VOTRE VIE PRIVÉE

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.

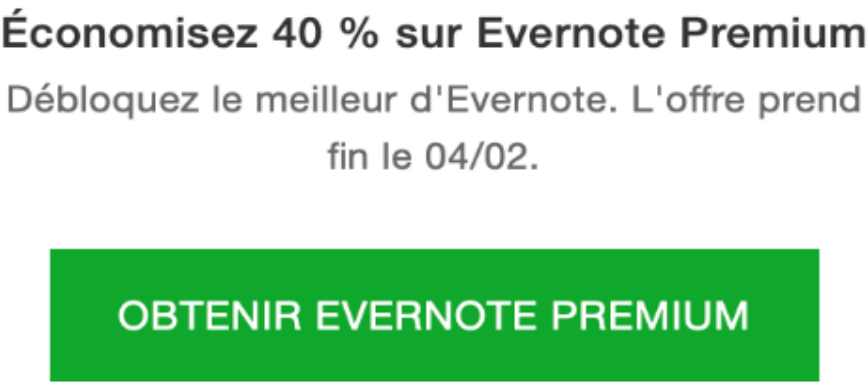
Obscurcissement : Rendre plus difficile la localisation des outils qui nous permettent de protéger notre vie privée.

- 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 :



BSCURCISSEMENT :

PRESSION :

Comment la méchante Reine peut-elle pousser Blanche-Neige à accepter des cookies « empoisonnés »?

Donnez un exemple de **chaque type d'interface truquée** qu'elle pourrait utiliser :

DOCUMENT D'ACCOMPAGNEMENT

MARKETING EN LIGNE DESTINÉ AUX JEUNES : PROTÉGEZ VOTRE VIE PRIVÉE

Les applications pour enfants les plus populaires

D'après le sondage *Jeunes Canadiens dans un monde branché* mené par HabiloMédias, les applications sur lesquelles les jeunes Canadiens de la 4e à la 11e année sont les plus susceptibles d'avoir un compte :

YouTube
(60 % ont un compte)

Facebook
(57 % ont un compte)

TikTok
(54 % ont un compte)

Instagram

Snapchat
(41 % ont un compte)

X (anciennement Twitter)

Amazon
(28 % ont un compte)

WhatsApp
(27 % ont un compte)