ccèsTI
AÎNÉS
2.0

SADC
Société
d'aide au développement
des collectivités
SHAWINIGAN

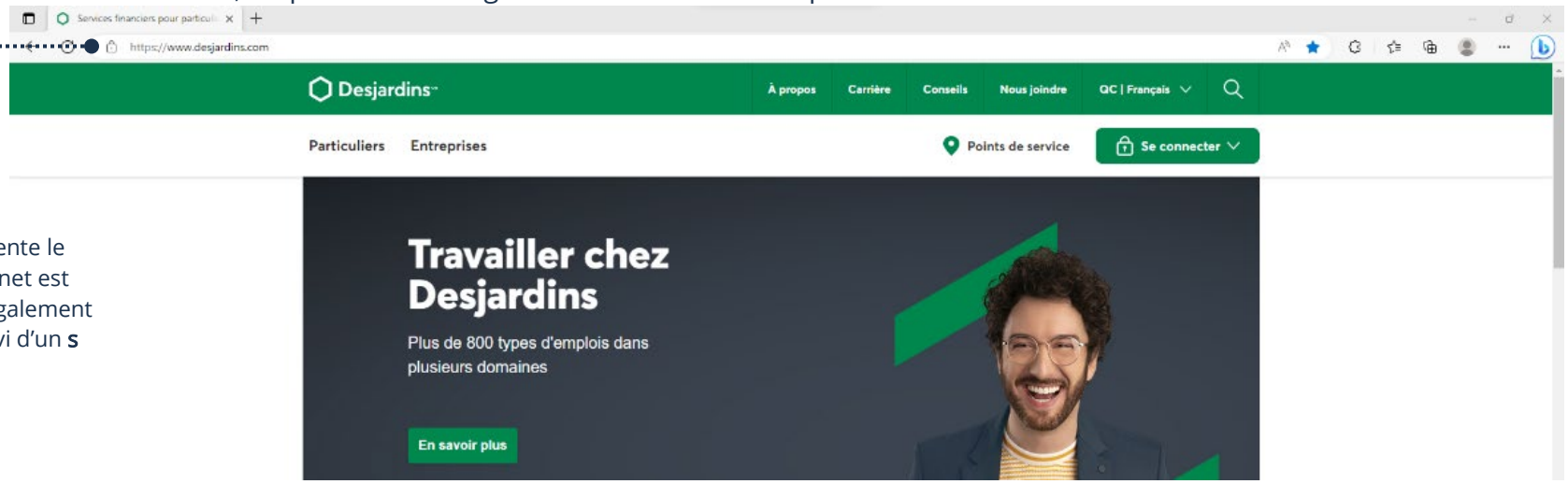
Thème 10
J'utilise sécuritairement et efficacement Internet

Navigateur Internet

Pour naviguer de façon sécuritaire, notamment lorsqu'on parle de transactions bancaires, il y a des éléments que vous pouvez vérifier afin de vous assurer que vous êtes sécuritaire sur Internet.

Reconnaître un site sécurité

Afin de vérifier si un site est sécurisé, un petit cadenas figurera dans la barre indiquant le site internet :



Ce cadenas représente le fait qu'un site Internet est sécurisé. Vérifiez également que le http soit suivi d'un **s** donc : https

Si le cadenas n'est pas présent, il peut s'agir d'un site Internet recréé pour ressembler à l'original. Il est donc important d'être vigilant!

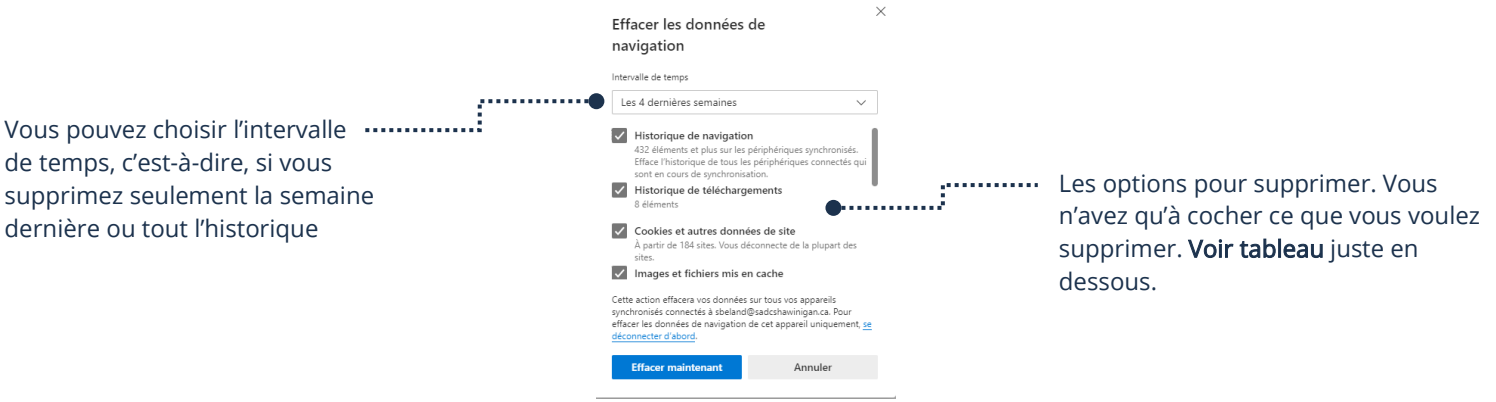
Si vous recherchez le site Internet directement sur Google, les chances de tomber sur un site officiel frauduleux sont moins grandes. Le danger, c'est de cliquer sur des liens dans les courriels par exemple. Dans le doute, recherchez un site Internet par vous-même à la place d'utiliser des liens. Vous aurez moins de chance de vous faire avoir. Également, attention aux sites de ventes douteux, renseignez-vous!

Suppression de l'historique de navigation

Vous pouvez supprimer l'historique de navigation de votre navigateur. Le but est de limiter l'accès à vos informations.

1. **Ouvrez** votre navigateur Internet
2. Cliquez sur **les trois petits points** en haut à droite de la page de votre navigateur
3. Sélectionnez **Historique**

4. Sélectionnez **Effacer l'historique de navigation**, cette fenêtre apparaîtra :



5. **Cochez** les options désirées et cliquez sur **Effacer maintenant**

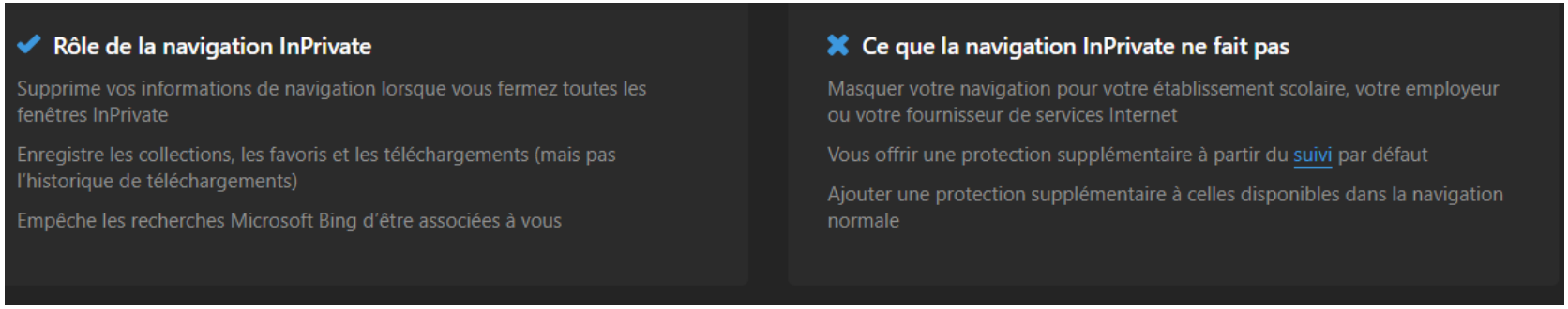
Historique de navigation	Il s'agit des pages Internet que vous avez visitées.
Historique de téléchargements	Il s'agit du site où vous avez téléchargé quelque chose.
Cookies et autres données de site	Il s'agit de données enregistrées pour la publicité, vos préférences, etc.
Images et fichiers mis en cache	Il s'agit d'images et fichiers sauvegardés qui accélèrent l'ouverture d'une page Internet.
Mot de passe	Vos mots de passe enregistrés lors de connexion sur un site Internet.
Remplissage automatique des données de formulaire	Les données entrées dans un formulaire sont enregistrées.
Autorisation des sites	Les autorisations que vous avez acceptées sur Internet.
Toutes les données de la version précédente de votre navigateur	Les données enregistrées par des versions précédentes du navigateur.
Données de média	Les licences et certificats des sites Internet visités.

Tous les navigateurs sont différents, mais ont les mêmes options. Vous pourrez donc vous y retrouver facilement. Dans le doute, vous pouvez cocher toutes les cases d'options pour la suppression. Toutefois, vous devrez entrer de nouveau vos mots de passe lors de votre prochaine visite sur un site Internet.

Navigation privée

Il est possible d'ouvrir une page de navigation privée. Le principal avantage est qu'aucun historique de navigation, ou mot de passe ne sera enregistré et ils se supprimeront automatiquement dès la fermeture du navigateur. C'est particulièrement utile si vous devez vous connecter sur un appareil qui n'est pas à vous.

1. **Ouvrez** votre navigateur Internet
2. Cliquez sur les **trois petits points** en haut à droite de la fenêtre
3. Sélectionnez **Nouvelle fenêtre de navigation privée** ou **Nouvelle fenêtre InPrivate**, selon votre navigateur
4. Une nouvelle fenêtre de votre navigateur apparaîtra et vous expliquera ce qui est enregistré et ce qui ne l'est pas :



5. Vous pouvez procéder et utiliser votre navigateur de la même manière que d'habitude

La navigation en privé est très utile lorsque vous magasinez. En effet, les cookies ne seront pas enregistrés et vous n'aurez pas de publicités en lien avec vos recherches pour acheter lorsque vous naviguerez sur Internet.

Les antivirus

- Les antivirus offrent une protection à votre appareil et vos données. Il y en a des versions gratuites et des versions payantes. Les versions gratuites sont de base et elles offrent moins d'options que les payantes. Cependant, les versions gratuites sont tout de même utiles et bonnes, tout dépend de vos besoins. Le but d'un antivirus est de bloquer des menaces et d'analyser votre appareil afin de protéger votre appareil et vos données.

Choisissez votre antivirus

Plusieurs options sont disponibles. Il est important de choisir un antivirus réputé offert par des entreprises. Conséquemment, ils sont donc un ajout de votre part à votre système. Windows dispose d'un antivirus de base, **Windows Defender**, mais ce n'est qu'avec un antivirus que vous aurez une protection supérieure.

Versions gratuites		Versions payantes	
Avira	https://www.avira.com	**Bitdefender**	https://www.bitdefender.com

Avast https://www.avast.com **Kaspersky** https://www.kaspersky.com

Utilisation d'un antivirus

Afin d'analyser votre appareil, vous devez utiliser votre antivirus. Ils sont tous semblables, vous vous y retrouverez peu importe celui que vous choisirez.

1. **Ouvrez** l'antivirus
2. Sélectionnez **Analyse de mon ordinateur** ou **Scan**
3. Une fenêtre apparaîtra vous indiquant le progrès de l'analyse.
4. Plusieurs minutes, jusqu'à une heure peuvent être nécessaires à l'antivirus pour compléter l'analyse
5. Si l'antivirus trouve une menace, vous pourrez alors la supprimer

Mises à jour

Il est très important de tenir l'antivirus à jour.

1. Ouvrez l'antivirus
2. Sélectionnez **Mettre à jour** ou **Mise à jour**

Vous pouvez également vérifier avec votre fournisseur Internet s'ils offrent un antivirus gratuitement avec votre service Internet. Ils pourront vous guider afin de l'obtenir s'il est offert.

Le Wifi

Pour ne pas être encombrés de câbles, nous avons de plus en plus recours au Wifi. Le Wifi permet de se connecter à Internet en utilisant des ondes. Il y a cependant deux types de Wifi :

- Wifi privé
- Wifi public

Le Wifi privé

C'est le plus commun. Il s'agit du Wifi que nous avons à la maison. Nous l'appelons Wifi privé parce qu'il faut, entre autres, un mot de passe afin d'y accéder. Il n'est donc pas accessible à tous et il est résidentiel. Il est plus sécuritaire parce qu'une personne mal intentionnée ne pourra pas facilement avoir accès à votre réseau et il est plus isolé. C'est pourquoi il est important de bien protéger son mot de passe Wifi et ne pas l'afficher au mur où il est possible de le voir par la fenêtre par exemple.

Le Wifi public

Le Wifi public est défini par son accessibilité et il n'est pas sécurisé. C'est le type de Wifi offert, par exemple, dans les hôtels et les restaurants. Étant donné qu'il est public, vous n'avez pas besoin d'un mot de passe pour y accéder ou le mot de passe est donné à tous les clients. C'est pratique, mais également une opportunité pour des gens mal intentionnés d'intercepter les informations auxquelles vous accèderez. C'est tentant pour ceux-ci, car ils savent qu'il y aura beaucoup d'appareils, possiblement mal protégés, accessibles sur le réseau.

Pour vous protéger sur un réseau public

- Il faut éviter d'aller sur des sites qui demandent des informations sensibles sur un réseau public. Ex : la banque
- Il faut éviter de se connecter à quoi que ce soit qui nécessite d'entrer un mot de passe. En effet, s'ils ont un mot de passe de votre part, ils peuvent essayer de se connecter à vos autres comptes. C'est pourquoi il est important d'utiliser un mot de passe différent pour chaque compte.
- Si vous n'avez pas le choix d'utiliser un réseau public, prévoyez un abonnement pour un VPN. Le VPN (Réseau privé virtuel) cryptera vos données, les rendant très difficiles à intercepter. Les VPN sont faciles à trouver grâce à une recherche sur Google

Si vous devez accéder à votre service bancaire et que vous n'avez comme option de connexion qu'un réseau public, il est préférable de tout simplement communiquer avec votre banque par téléphone pour faire vos transactions s'il s'agit d'une urgence ou d'attendre d'être à la maison.

Prenez garde!

Les gens mal intentionnés sur Internet ont une multitude de stratégies afin de frauder ou usurper vos informations. La plupart sont constantes pour ne pas dire standard et facilement reconnaissables pour l'usager averti. Ces stratégies utilisent toutes une faiblesse de la psyché humaine afin de vous inciter à agir. Vous pouvez éviter de tomber dans le piège en étant vigilant, logique et en portant une attention particulière aux :

- Ventes frauduleuses
- Publicités frauduleuses
- Courriels indésirables
- Faux concours
- Fausses nouvelles
- Publications demandant des informations par voies indirectes

Ventes frauduleuses

Prenez garde lors des transactions. Comme dans n'importe quel domaine, des gens mal intentionnés peuvent essayer de vous frauder. N'envoyez pas d'argent avant d'avoir vu l'article et être en mesure d'aller le chercher. Attention également si le vendeur vous **demande un montant d'argent à l'avance (dépôt).** Il arrive que vous envoyiez de l'argent et n'entendiez plus parler du vendeur. C'est pourquoi il est préférable de payer **une fois sur place**. Si le vendeur ne veut pas et insiste pour un paiement à l'avance, il est souvent préférable de simplement laisser tomber et chercher de nouveau votre article pour faire affaire avec un autre vendeur. Également, **ne donnez pas d'informations personnelles**. Exemple : les numéros de votre carte de crédit. Il est aussi préférable de **vous déplacer à deux**. De cette façon, quelqu'un sera avec vous et vous aurez un témoin.

Publicités frauduleuses

Il faut faire attention avec les publicités qui offrent des solutions **trop belles pour être vraies**. Par exemple, si une offre mentionne que tous les gens de Shawinigan font 100 000 $ par année en suivant un truc et en cliquant sur le lien ou encore, une artiste populaire a perdu 50 kg grâce à cette pilule. Ce type de publicité est souvent ce qui est appelé en anglais un "Click Bait". Le but étant de vous **inciter à cliquer,** car c'est tentant. Dites-vous bien que, dans nos exemples précédents, on en entendrait parler à la télé si c'était si facile! Il s'agit souvent d'une ruse afin d'obtenir vos informations et vous frauder ou infecter votre système.

Lorsque vous **ressentez du stress ou de l'inquiétude** à propos de votre ordinateur, il est important de bien réfléchir ou de **demander conseil**. La plupart des pièges sur Internet fonctionnent lorsqu'une personne agit rapidement sous la **peur ou l'inquiétude.**

Courriels indésirables

Votre boîte de courriel **filtrera automatiquement** certains courriels reçus. Plusieurs de ces courriels sont reconnus par un algorithme et les signes d'un courriel problématique par l'entreprise vous offrant le service et seront **envoyés directement dans la boîte de courriels indésirables**. Il arrive cependant que des messages frauduleux ou non désirés **se glissent dans votre boîte de réception**. Il est **important** de ne pas :

- **Ouvrir** un courriel indésirable
- **Suivre un lien** venant d'un courriel indésirable ou dont on ne connaît pas la provenance
- **Répondre** à un courriel indésirable ou un courriel frauduleux

La meilleure solution reste de tout simplement **le supprimer** et ne pas en tenir compte. En effet, certains courriels sont conçus de façon à **attirer votre attention par un sentiment d'urgence et/ou de gravité de la situation**. Si, par exemple, vous avez un courriel spécifiant un problème

avec un compte bancaire, n'utilisez pas le courriel pour répondre ou suivre un lien. Il est **préférable de communiquer** directement avec votre banque. Ils pourront vous indiquer s'il y a un problème ou non. Vous pouvez faire la même chose pour **tous vos comptes.**

Voici quelques stratagèmes utilisés afin d'obtenir vos informations :

- Courriel qui **semble officiel**. Ex : Gouvernement
- Courriel qui mentionne que vous êtes en état d'arrestation
- Courriel mentionnant un problème et qui réclame de suivre un lien et de vous connecter
- Courriel mentionnant un problème et demande un montant en argent pour le régler

Il est important de **ne pas paniquer** et de réfléchir sur une façon de **vérifier l'information** reçue en passant par autre chose que le courriel. En paniquant, vous risquez d'agir impulsivement et de tomber dans le piège. Vous verrez, il s'agit souvent d'une arnaque. C'est quand même bien de vérifier!

Faux concours

Les faux concours se présentent souvent sur des plateformes comme Facebook. Il s'agit d'un concours, souvent tentant, où on vous demande de participer et d'envoyer vos informations personnelles. Le problème est que vous ne gagnerez jamais, car **le but est simplement d'obtenir vos informations**. Si vous souhaitez participer à des concours, il vaut mieux **vérifier l'information** d'abord. Par exemple, vous pouvez effectuer une recherche et aller sur le **site Internet officiel** de l'entreprise ou de l'organisme. S'il y a bel et bien un concours, il y sera officialisé. Si vous ne trouvez pas d'information à propos du concours, il est généralement **plus sage de simplement l'ignorer.**

Fausses nouvelles

Les fausses nouvelles sont tout simplement des nouvelles ou des articles communiquant **des informations erronées ou non prouvées**. Le problème est qu'elles peuvent être très convaincantes. Elles sont ce qu'on appelle en anglais des "Click Bait" ou en français des appâts pour vous faire ouvrir la page Internet. Le but de ces nouvelles n'est pas de vous informer, mais de créer de l'achalandage sur le site Internet afin de provoquer des profits publicitaires. **Effectuer une recherche pour confirmer** les propos d'une nouvelle qui ne vient pas d'une source officielle est le **meilleur moyen de s'assurer de la véracité** de l'information.

Publications demandant des informations personnelles par voies indirectes

Souvent sur Facebook, ce type de publication a pour but d'obtenir des informations personnelles. On parle ici de voies indirectes parce que ce n'est pas spécifiquement indiqué de remettre des informations.

- Ex : une publication demande candidement quelle est la dernière photo que vous avez de votre animal. Les gens vont alors publier dans les commentaires une photo de leur animal ainsi que son nom. Cependant, c'est connu par les fraudeurs qu'un mot de passe très courant est le nom d'un animal vous appartenant. Ils ont ainsi un indice et peuvent tenter de prendre possession de vos comptes.

Ce type de demande peut prendre plusieurs formes. Quelle est votre ville de naissance? Dites-nous votre plat préféré. Etc. Les variations sont nombreuses. Afin de ne pas tomber dans le piège et dans le doute, il vaut mieux ne pas répondre. Moins vous en indiquez sur Internet, plus vous êtes protégé!

Reconnaître un site officiel

- Les fraudeurs et les gens mal intentionnés ont souvent recours à de faux sites Internet ou encore de fausses pages officielles. Ils vont alors recréer un site Internet ou une page de toute pièce pour vous berner.
-

Vous pouvez regarder plusieurs petites choses afin de vous assurer de l'authenticité d'un site Internet. Vous avez entre autres le petit cadenas à la barre d'adresse ou encore le https. Cependant, il arrive que les fraudeurs soient créatifs. Afin de ne pas vous faire avoir :

- **Vérifiez l'orthographe**. Souvent, les sites Internet frauduleux créés pour ressembler aux sites officiels seront remplis d'erreurs de français.
- **Vérifier le bas de la page Internet**. Les sites officiels vous donnent plusieurs informations que les sites frauduleux ne donnent pas :

Vous y avez les informations pour communiquer avec la compagnie et les mentions légales. Si **les liens fonctionnent** et les numéros de téléphone sont véridiques, c'est bon signe. Les fraudeurs n'ajouteront généralement pas ces informations parce qu'ils ne veulent pas que vous communiquiez avec la banque. Leur stratagème échouerait automatiquement.

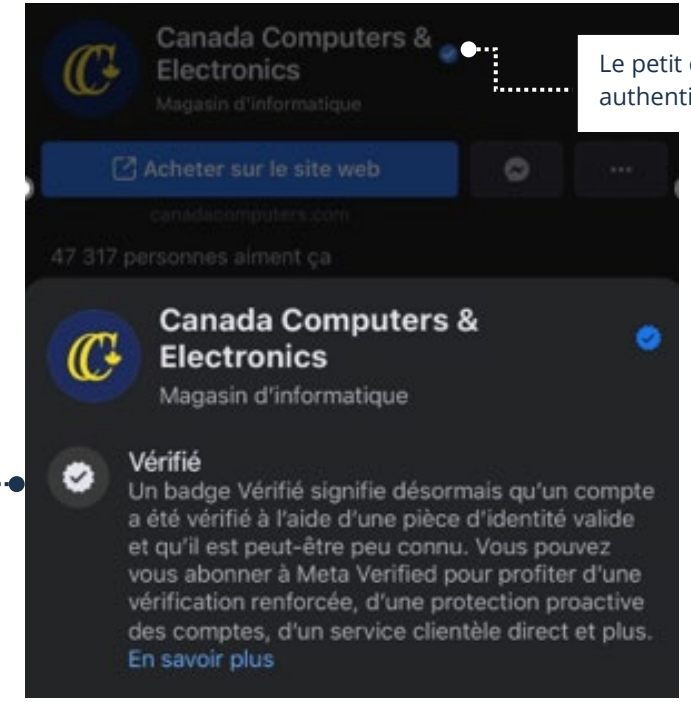
Infos utiles

Les moteurs de recherche font généralement un très bon travail afin de toujours vous envoyer sur le site officiel de votre recherche. Tant qu'il s'agit d'une compagnie connue, vous tomberez à 99% sur le site officiel. Ils ont des mesures de sécurité intégrées afin de filtrer les sites Internet frauduleux.

Reconnaître une page Facebook officielle

Facebook a un protocole en place afin de confirmer l'authenticité d'une page officielle. Un responsable d'un organisme ou d'une compagnie peut prouver à Facebook que c'est la vraie page. Il s'agit d'un **badge vérifié** situé à côté du nom de la compagnie ou de l'organisme sur la page officielle :

Facebook vous indique que c'est vérifié si vous cliquez sur le petit crochet.



Le petit crochet encerclé de bleu indique que la page fut authentifiée comme étant authentique

Signalement d'une publication Facebook

- Il arrive de voir des publications inappropriées sur Facebook. Que ce soit de la fraude, des insultes, des sujets scabreux, etc. Il est possible de les signaler à Facebook afin de les faire retirer.

Signalement d'une publication

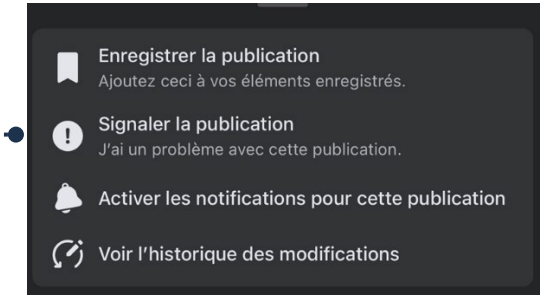
Pour signaler une publication :

1. Cliquez sur les **trois petits points** situés dans le coin supérieur droit de la publication

Les trois petits points représentent plus d'options

2. Une fenêtre apparaîtra contenant **un menu vous permettant de signaler**

Touchez et suivez les étapes



3. Sélectionnez **Signaler la publication** et suivez les étapes. Facebook pourra alors agir en conséquence.