ccèsTI
AÎNÉS
2.0

SADC
Société
d'aide au développement
des collectivités
SHAWINIGAN

Thème 10 - Intermédiaire
J'utilise sécuritairement et efficacement Internet

Les cookies

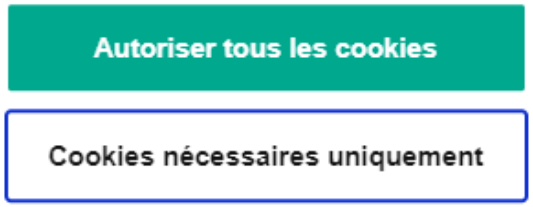
Les cookies sont **des témoins** et **des données de sites Internet**, sous un format de fichiers textes.

Tout le monde ou presque a déjà vu **une bannière en bas ou en haut d'une page Internet** qui demande **une autorisation pour les cookies**. Ils peuvent contenir une personnalisation du site, des données de connexions, etc. Quand nous acceptons d'enregistrer ce petit fichier dans notre appareil, chaque site Internet décide de sa bannière et des choix offerts dans celle-ci.

Autorisation d'enregistrement des cookies afin d'y accéder

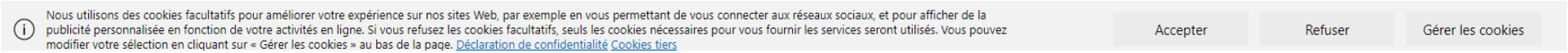
Certains sites **obligent l'enregistrement** des cookies afin d'y accéder.

D'autres sites vous permettront d'accepter tous les cookies, ou **seulement ceux obligatoires**.



Refus d'enregistrement des cookies

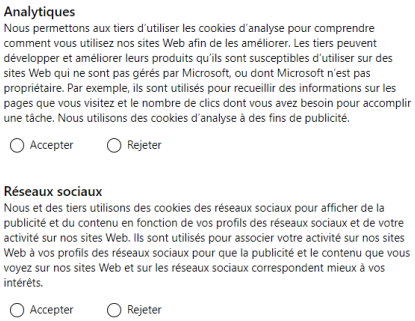
Certains sites permettent **de refuser** les cookies.



Il est important de prendre note que **refuser des cookies peut compromettre votre accès au site Internet**. Il arrive qu'un refus vous **empêche de consulter le site Internet.**

Gestion de l'enregistrement des cookies

Certains sites permettent **la gestion de l'enregistrement des cookies**. En sélectionnant **Gérer**, vous pouvez **décider** ce que vous **acceptez ou refuser** de sauvegarder.

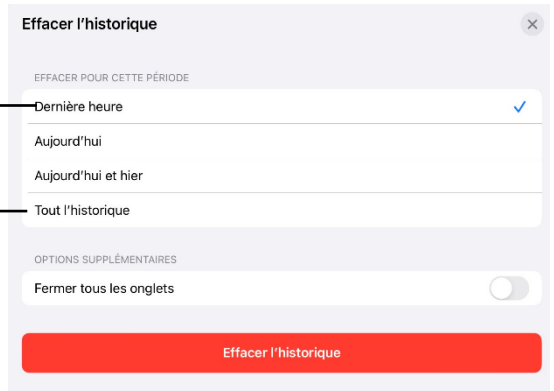


Suppression des cookies

Supprimer les cookies enregistrés dans le navigateur Internet de votre appareil peut vous **aider à réduire les risques de violation de votre vie privée**. Cependant, toute personnalisation (langue, ville, etc.) sur le site **sera également supprimée**.

1. Ouvrez votre **navigateur Internet** (Safari)
2. Touchez **l'icône du menu** en haut à gauche 
3. Touchez **Historique** → **Effacer** (effacer se trouve en bas du menu), une fenêtre apparaîtra :

Permet de choisir la période pour laquelle vous souhaitez supprimer l'historique de navigation ainsi que les témoins (Cookies)

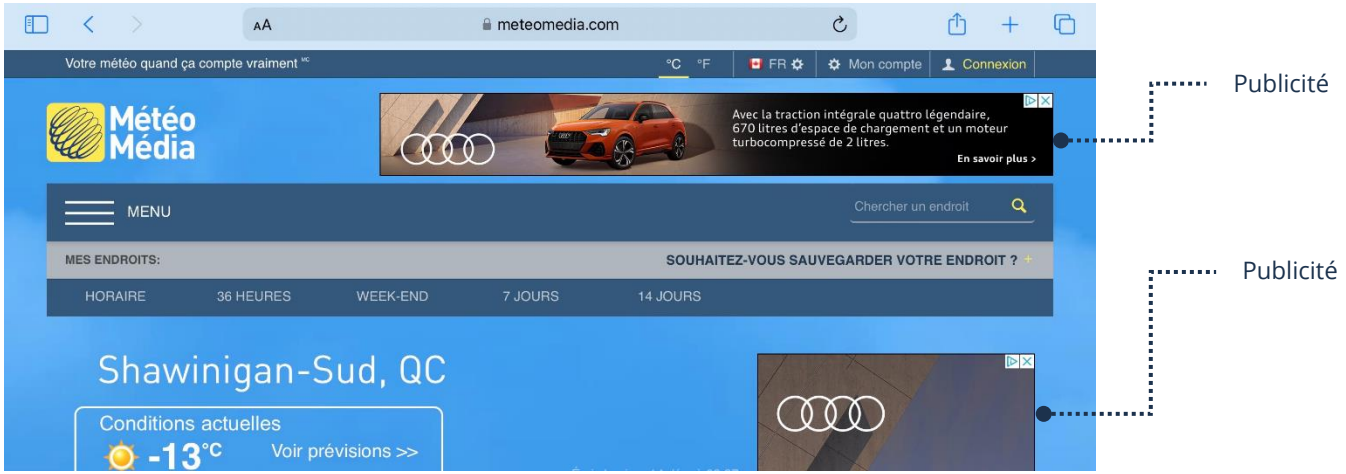


4. Une fois la sélection de la période faite, touchez **Effacer l'historique**

Les publicités

Reconnaître une publicité

Une des plus faciles à reconnaître est la publicité affichée en haut, dans la bannière.



Les publicités **peuvent être grandes, petites, larges, etc.** Il existe plusieurs termes dans l'affichage des annonces publicitaires sur une page Internet. Les termes sont habituellement inscrits en bas, mais pas toujours. Il suffit **d'analyser** la page Internet avant de les toucher et avec le temps, vous les reconnaîtrez plus rapidement :

- Publicités
- Sponsors
- Annonces
- Liens commerciaux
- Services partenaires
- Un **X** sera affiché en haut de l'image (AdChoices)
- Etc.

Notez qu'il faut toujours **faire attention avec les publicités**, mais toucher afin d'ouvrir l'une d'elles est habituellement inoffensif s'il s'agit d'une publicité d'un magasin.

Virus

La plupart des virus se **font passer pour un logiciel ou une application officielle** afin d'inciter les gens à les exécuter/installer sur leur appareil et ainsi infecter le système. Une **pièce jointe à un courriel** peut contenir un virus, donc si vous ouvrez la pièce jointe, le risque d'infection est grand. Toutefois, il est important de comprendre que **la plateforme d'Apple, iOS, est très rigide. C'est cette rigidité qui rend les risques d'infections par des virus beaucoup moins importantes sur les produits Apple.** Cependant, vous **êtes à risque**, même sur un appareil Apple, si **vous installez vous-même** le logiciel malveillant **en tombant dans un piège**, comme un message sur Messenger contenant un lien qui mène à un virus ou encore, en ouvrant une pièce jointe d'un courriel indésirable.

Dans les rares cas où vous auriez un virus sur votre appareil Apple, une **réinitialisation complète de l'appareil** règle souvent le problème. Veillez à **bien sauvegarder vos données avant**, une réinitialisation est **irréversible** et efface tout de l'appareil. Vous devrez également **changer vos mots de passe et vous en souvenir**.

Démystifier les différents types de menaces informatiques

Malware	Appellation qui désigne tout type de logiciel malveillant. Un Virus est un type de Malware
Virus	Les virus informatiques sont des malwares qui doivent être déclenchés par l'utilisateur
Vers	Il est autonome et se propage vers d'autres appareils tout en restant actif sur tous les appareils qu'il infecte
Rançongiciels	Verrouille l'appareil de sorte que vous ne puissiez les ouvrir jusqu'à ce que payez la rançon
Chevaux de Troie	Souvent appelé par le terme anglais Trojan, se cache dans un logiciel que vous installez sur votre ordinateur et son objectif est bien souvent de voler vos informations bancaires
Publicités Malveillantes	Ces virus ont pour but de vous faire visionner un maximum d'annonces publicitaires
Logiciels espions	Souvent appelé par le terme anglais Spyware, il espionne vos données afin de les transmettre à la personne mal intentionnée
Rootkit	Conçu pour permettre à des pirates informatiques d'accéder à votre appareil afin de le contrôler
Keylogger	Tout ce que vous tapez sur votre clavier sera envoyé à la personne mal intentionnée afin d'avoir accès à vos informations bancaires et de mails

Installation d'un antivirus

1. Ouvrez l'application **App Store**
2. **Recherchez** l'antivirus
3. Touchez **Obtenir**

Comment savoir si j'ai été infecté

- Des fenêtres (pop-up) s'ouvrent avec des publicités
- La page d'accueil de votre navigateur Internet a changé alors que vous ne l'avez pas modifié
- Des courriels étranges envoyés à votre liste de contacts envoyée par votre compte
- L'appareil tombe souvent en panne avec peu d'application active
- L'appareil est lent même après un redémarrage
- Des applications inconnues démarrent au démarrage de l'appareil
- Vos mots de passe changent à votre insu

Faux Virus

Un virus est un logiciel ou une application malveillant codé afin de vous nuire. Un bon **antivirus peut vous aider** à vous protéger. Cependant, il existe **de fausses fenêtres (Pop-up)** qui vous font **croire** que vous êtes contaminé par un virus

Fenêtre (Pop-up) antivirus/infections

Les fraudeurs créent de **fausses fenêtres afin d'arnaquer les gens**. Ainsi, les gens cliquent dans une fenêtre ou touche **Réparation** pensant être infecté et ils se voient offrir l'achat d'un antivirus ou une aide immédiate, mais en fait le prétendu logiciel de sécurité (antivirus) **déclenche le téléchargement du logiciel malveillant**. De plus, si vous payez pour le prétendu logiciel de sécurité (antivirus) vous donnez vos informations de carte bancaire aux arnaqueurs. Voici **un exemple** et il est valide, peu importe l'appareil utilisé.

Cette fausse menace peut **prendre plusieurs formes**. Par exemple, nous avons le contrôle de votre appareil ou encore, problème bancaire, vous avez gagné un concours, etc. La meilleure façon pour un fraudeur d'obtenir vos informations, c'est de vous **faire tomber dans un piège**. Il n'y a **aucune** page Internet de ce genre **dont vous devez vous soucier**. Vous pouvez simplement **fermer cette page** et supprimer votre historique de navigation.

Comment savoir si c'est une fausse fenêtre d'alerte virale?

- Crée de la panique, car ils veulent que vous fassiez un achat impulsif. Les fournisseurs d'antivirus officiel ne s'y prennent pas de cette façon
- Conception graphique de la fenêtre qui ne fait pas toujours professionnel
- Contiennent souvent des fautes d'orthographe
- Souvent, les fausses fenêtres vous donneront un numéro de téléphone afin de les appeler et ainsi ils pourront créer davantage de paniques et vous soutirer de l'argent et vos informations bancaires

Paiements sur Internet

Il arrivera surement un moment où vous aurez l'envie d'acheter quelque chose en ligne. Que ce soit par carte de crédit ou par virement Interac, voici **quelques conseils** si vous faites un paiement sur Internet.

- Assurez-vous que votre appareil est à jour
- Faites attention aux sites qui ont des offres alléchantes et que vous ne connaissez pas
- Vérifiez l'identité du vendeur et sa réputation. Effectuez une recherche sur Google afin de vous y aider
- Vérifiez les mentions légales et les conditions générales de vente du site Internet
- Ne vous fiez pas seulement aux avis des consommateurs, car il peut s'agir de faux avis
- Vérifiez que la page est bien sécurisée
- Soyez vigilant lors du paiement
- N'enregistrez pas vos informations de paiements sur le site Internet
- Méfiez-vous des réseaux Wi-Fi publics
- Choisissez toujours la double authentification avec votre institution bancaire
- Consultez régulièrement votre compte bancaire

Sites de rencontres

Les rencontres en ligne sont maintenant rendues normalisées. Des millions de gens s'en servent afin de rencontrer l'amour ou simplement de la compagnie amicale. Ceci peut avoir **beaucoup de côtés positifs, mais il y a quelques risques** tout de même si vous décidez d'utiliser ceux-ci.

Les dangers des sites de rencontres

Harcèlement obsessionnel

Il pourrait arriver qu'une personne **n'aime pas se faire dire non**, il continuerait donc à envoyer des messages même après avoir indiqué ne pas être intéressé à échanger.

Les arnaques sentimentales

L'arnaqueur, **généralement un faux profil, amadoue, manipule, etc.,** l'autre personne dans le but de **gagner sa confiance**. Au fil du temps ils vont commencer à **demander de l'argent** ou finiront par obtenir les informations personnelles afin **d'usurper l'identité**.

Signes précurseurs dont vous devez vous méfier sur les sites de rencontres

- Vous demande rapidement de discuter sur une autre application
- La personne vous demande une aide financière en raison d'une situation personnelle difficile
- Prétends être veuf ou veuve depuis peu
- Vous bombarde de compliments exagérés dès le début de vos échanges
- Vous demande votre adresse sous prétexte d'un cadeau
- Raconte des histoires mélodrames sur eux-mêmes
- Affirme vivre dans notre pays, mais dit être présentement en voyage dans un autre pays, ce qui les empêche de vous téléphoner ou de vous rencontrer
- La personne disparait du site et revient sous un nouveau nom

Si vous décidez de rencontrer quelqu'un, pour les premières rencontres, il est impératif de **faire les rencontres dans un endroit public et de signaler, la date, l'heure et l'endroit à un(e) ami(e).** Lors du rendez-vous, apportez un cellulaire et demandez à votre ami(e) de vous appeler pendant la rencontre afin de s'assurer que tout se passe bien.

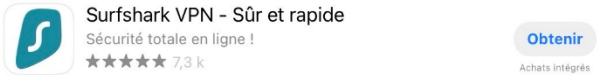
VPN

Un **Virtual Private Network, abrégé en VPN**, veut dire **réseau privé virtuel** en français. Pour faire simple, c'est un service qui permet de naviguer sur Internet de façon sécuritaire et qui permet de modifier sa localisation. Celui-ci cache l'adresse IP de l'utilisateur et son emplacement, donc le VPN offre **une navigation confidentielle** empêchant quiconque de connaître votre identité. De plus, les données circulent dans un **tunnel crypté**, rendant ainsi vos données sécurisées.

L'interface d'une application VPN est assez simple, généralement on y trouve :

- La liste des **pays** disponibles
- Le bouton **Connexion** et **Déconnexion**
- **Réglages** qui pour les néophytes ne sont pas obligés de changer quoi que ce soit

Il existe des versions gratuites et d'autres payantes. Cependant, les versions gratuites sont parfois lentes quand vous naviguez sur Internet. Si vous voyagez ou vous pensez utiliser souvent l'application, il vaut peut-être mieux investir dans un bon VPN.



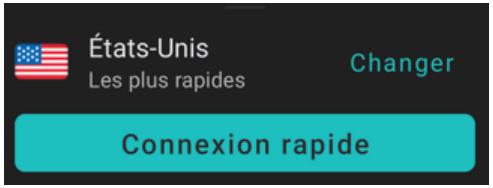
Installation d'un VPN

1. Ouvrez l'application **Apple Store**
2. **Recherchez** le VPN
3. Touchez **Obtenir**

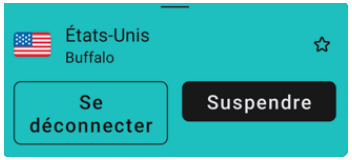
Généralement un VPN demande la création d'un compte afin d'utiliser le service et si c'est une version payante, il vous sera demandé les infos de paiements. **Veuillez noter que certains antivirus payants incluent un VPN**.

Connexion/Déconnexion d'un VPN

1. Ouvrez votre **application VPN**
2. **Choisissez votre pays** de connexion, le pays choisi sera l'emplacement de localisation et touchez **Connexion**



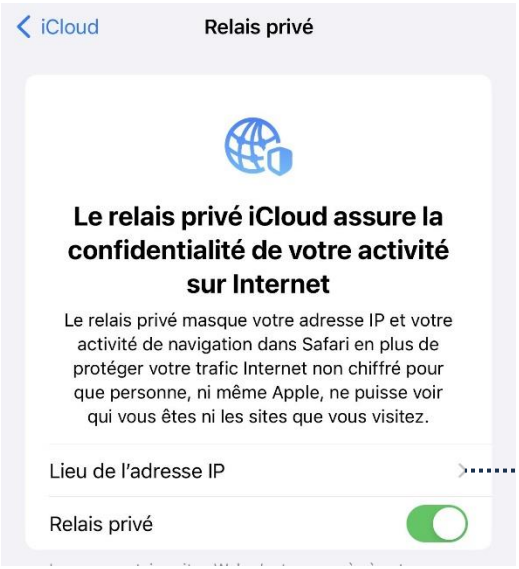
3. Naviguez sur Internet comme **vous faites habituellement**
4. Quand vous **ne voulez plus utiliser** le VPN, touchez **Déconnexion** ou **Se déconnecter**

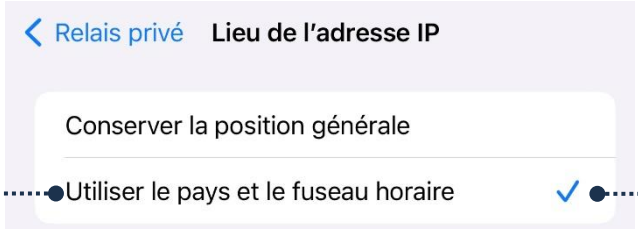


Le relais privé d'Apple

Si vous possédez un **abonnement à Apple One ou iCloud+**, vous pouvez activer un service d'Apple qui **sert de complément**, pour le moment, à un VPN. Ce service ne fonctionne **qu'avec le navigateur Internet Safari**. Afin **d'activer** le Relais privé (Private Relay en anglais) d'Apple :

1. **Réglages → Votre compte → iCloud → Relais privé**





Permet d'augmenter les choix et la distance pour l'adresse sous laquelle vous naviguerez sous la protection du Relais privé

2. Touchez **le taquet** du Relais privé afin de **l'activer**