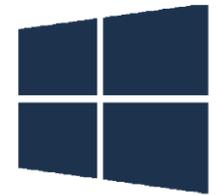




ccèsTI
AÎNÉS
2.0



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 données de sites Internet**.

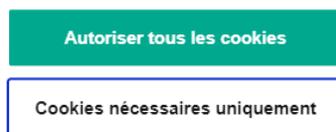
Tout le monde ou presque a déjà vu **une bannière en bas ou en haut d'une page Internet** qui demande **une autorisation pour les cookies**. Les cookies **sont des fichiers textes** qui peuvent contenir une personnalisation du site, des données de connexions, etc. Quand nous acceptons d'enregistrer ce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

Autorisation d'enregistrement des cookies

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

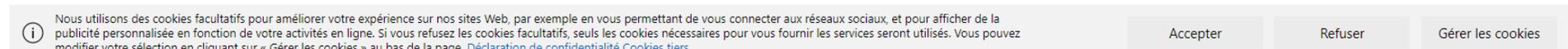
Ce site utilise des cookies provenant de Google afin de fournir ses services, d'en améliorer la qualité et d'analyser le trafic. [En savoir plus](#) [J'ai compris](#)

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 refusez** de sauvegarder :

Analytiques

Nous permettons aux tiers d'utiliser les cookies d'analyse pour comprendre comment vous utilisez nos sites Web afin de les améliorer. Les tiers peuvent développer et améliorer leurs produits qu'ils sont susceptibles d'utiliser sur des sites Web qui ne sont pas gérés par Microsoft, ou dont Microsoft n'est pas propriétaire. Par exemple, ils sont utilisés pour recueillir des informations sur les pages que vous visitez et le nombre de clics dont vous avez besoin pour accomplir une tâche. Nous utilisons des cookies d'analyse à des fins de publicité.

Accepter Rejeter

Réseaux sociaux

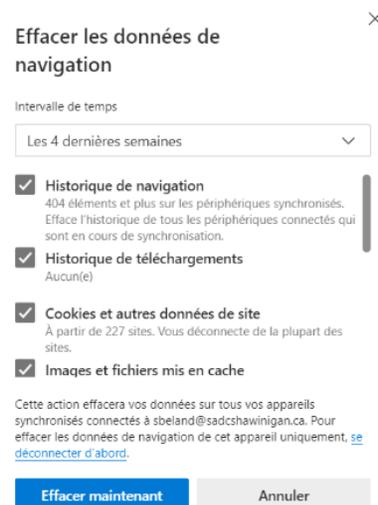
Nous et des tiers utilisons des cookies des réseaux sociaux pour afficher de la publicité et du contenu en fonction de vos profils des réseaux sociaux et de votre activité sur nos sites Web. Ils sont utilisés pour associer votre activité sur nos sites Web à vos profils des réseaux sociaux pour que la publicité et le contenu que vous voyez sur nos sites Web et sur les réseaux sociaux correspondent mieux à vos intérêts.

Accepter Rejeter

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
2. Cliquez sur les **trois petits points** en haut à droite 
3. Cliquez sur **Historique** → **Effacer les données de navigation** ou **l'icône de la poubelle** (selon le navigateur que vous utilisez)

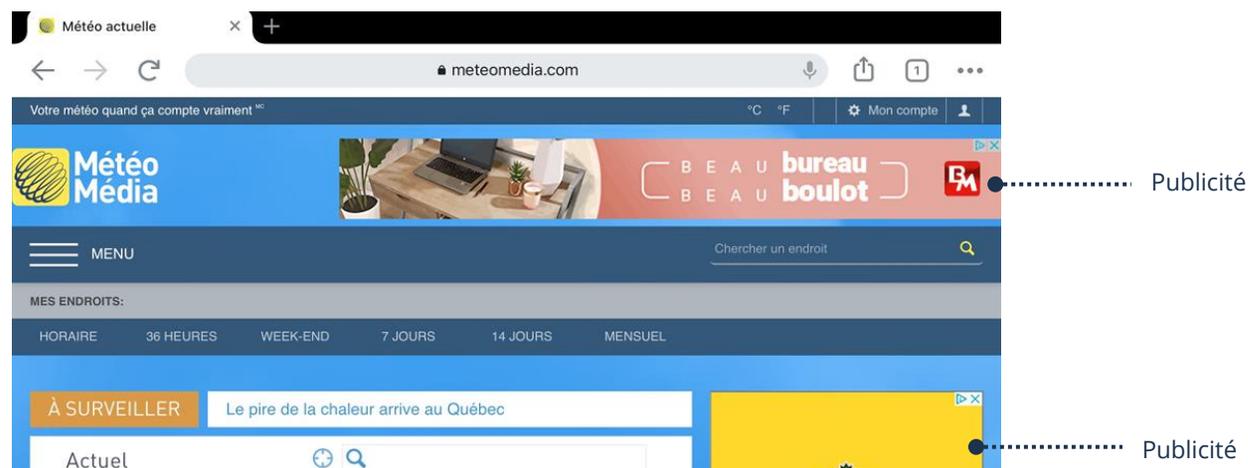


4. Assurez-vous que les cases **Cookies et autres données de site** soient bien cochées
5. Cliquez sur **Effacer maintenant** pour supprimer les cookies

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
- Commandités
- Annonces
- Lien commercial
- Service partenaire
- Un X sera affiché en haut de l'image (AdChoices)
- Etc.

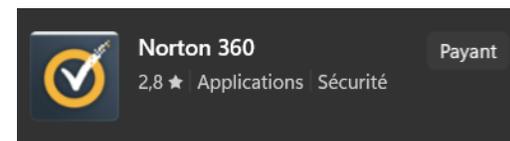
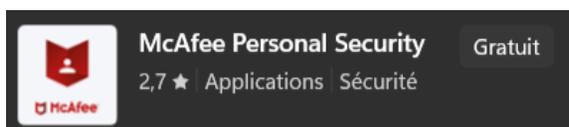




Notez qu'il faut toujours **faire attention avec les publicités**, mais toucher afin d'ouvrir l'une d'elles est habituellement inoffensif s'il s'agit d'une publicité d'un magasin.

Virus

La plupart des virus se **font passer pour un logiciel ou une application officielle** afin d'inciter les gens à les exécuter sur leur appareil et ainsi installer le virus qui aura une fonction spécifique. Sinon, les autres virus vont **opérer de façon incognito** afin de tenter d'obtenir vos informations. Une **pièce jointe à un courriel** peut contenir également un virus, donc si vous ouvrez la dite pièce jointe infectée, vous installez le virus. **En installant un antivirus**, cela peut vous aider grandement.



Installation d'un Antivirus

1. Choisissez un antivirus	Il existe de nombreuses options disponibles sur le marché. Faites des recherches pour trouver celui qui correspond le mieux à vos besoins et à votre budget.
2. Téléchargez l'antivirus	Rendez-vous sur le site web de l'antivirus que vous avez choisi et téléchargez le programme d'installation en cliquant sur Télécharger
3. Exécutez le programme d'installation	Une fois le téléchargement terminé, double-cliquez sur le fichier d'installation pour démarrer le processus d'installation
4. Suivez les instructions à l'écran	L'assistant d'installation vous guidera tout au long du processus. Acceptez les conditions d'utilisation, choisissez les options de configuration selon vos préférences et cliquez sur " Suivant " ou " Installer " pour démarrer l'installation.
5. Attendez la fin de l'installation	L'installation peut prendre quelques minutes. Laissez le programme s'installer complètement et cliquez sur Terminer

6. Redémarrez votre ordinateur

Il est nécessaire de **redémarrer votre ordinateur** pour finaliser l'installation de l'antivirus



Assurez-vous de télécharger l'Antivirus depuis une source fiable pour éviter les logiciels malveillants

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 **Microsoft Store**
2. **Recherchez** l'antivirus
3. Cliquez sur **Gratuit ou Payant**, selon le cas

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 modifiée
- Des courriels étranges envoyés à votre liste de contacts, le tout envoyé par votre compte
- L'appareil tombe souvent en panne avec peu d'applications actives
- 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 malveillante, codés 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 :

Votre système est lourdement endommagé par (quatre) virus!

Nous détectons que votre Samsung Galaxy S6 est 28,1% endommagé en raison de (quatre) virus nocifs provenant de sites récents adultes. Bientôt il va endommager la carte SIM de votre téléphone et corrompre vos contacts, les photos, les données, les applications, etc.



Si vous ne supprimez pas le virus maintenant, il causera de graves dommages à votre téléphone. Voici ce que vous devez faire (étape par étape):

Étape 1: Appuyez sur le bouton et installer APP gratuitement sur Google Play!

Étape 2: Ouvrez l'application pour accélérer et fixer votre navigateur maintenant!

RÉPARATION RAPIDE MAINTENANT

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 communiquer avec les fraudeurs et ils pourront ainsi créer davantage de panique et vous soutirer de l'argent et vos informations bancaires

Paielements sur Internet

Il arrivera sûrement 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.



Facebook Rencontres



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 disparaît 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.

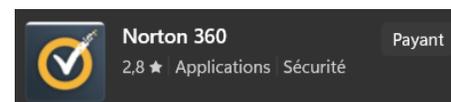
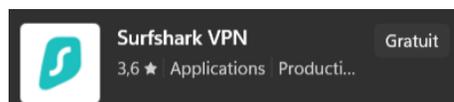
VPN

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

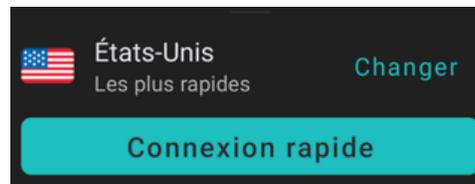
1. Ouvrez **Microsoft Store**
2. **Recherchez** le VPN
3. Cliquez sur **Gratuit ou Payant**, selon le cas



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. **Veillez 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 cliquez sur **Connexion**



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

