SYNDESIN
ACCOMPAGNEMENT NUMERIQUE

Mes fiches mémos

INTRODUCTION

Avez-vous déjà remarqué l'affichage d'une publicité vous présentant un produit que vous aviez consulté sur un site Internet quelques jours auparavant ? Ou bien que l'un de vos proches partageait peut-être un peu trop d'informations privées sur les réseaux sociaux ? La sensibilisation aux menaces liées à une mauvaise utilisation d'Internet est donc indispensable.

Nous vous invitons à découvrir 8 réflexes à adopter pour naviguer sur Internet en évitant les principales menaces, telles que l'hameçonnage (phishing en anglais), l'infection par un virus ou encore le piratage de comptes pouvant mener jusqu'à une usurpation d'identité.

AYEZ TOUJOURS UN NAVIGATEUR A JOUR

Il est essentiel de garder son système d'exploitation et ses logiciels à jour comme son navigateur (Google Chrome, Mozilla Firefox, Internet Explorer, Safari ou Opera par exemple). Des failles de sécurité peuvent être exploitées lorsqu'ils ne le sont pas.

Dès que votre navigateur vous le propose, **faites donc ces mises à jour essentielles à votre sécurité sur le web**. Lorsque cela est possible, n'hésitez pas à activer les mises à jour automatiques.

NAVIGUEZ SPONTANEMENT EN MODE "PRIVE"

Tous les navigateurs web possèdent un mode "incognito" ou "privé". Son principal intérêt consiste à ne pas enregistrer l'historique de navigation sur votre appareil. Le deuxième intérêt est de limiter l'envoi d'informations aux sites Internet sur lesquels vous naviguez. Si cela est possible, activez l'ouverture automatique en navigation privée dans les réglages de votre navigateur ou **dès que vous naviguez sur Internet**.

Notez également naviguer sur Internet de façon privée a un intérêt supplémentaire : certains sites peu scrupuleux utilisent les "**cookies**" pour adapter leurs tarifs à votre comportement de navigation.

Un cookie est un fichier qui est déposé par votre navigateur sur votre ordinateur lorsque vous naviguez sur Internet. Ce fichier enregistre des informations personnelles vous concernant, comme l'âge, votre pseudo sur un site Internet ou bien des habitudes de consommation. Ces informations sont ensuite collectées et analysées pour améliorer votre navigation, mais aussi et surtout pour vous proposer des publicités ciblées sur votre profil. Naviguer sur Internet en mode privé permet de ne pas conserver ces fichiers lorsque vous fermez le navigateur.

CONFIGUREZ VOTRE NAVIGATEUR POUR INDIQUER QUE VOUS REFUSEZ D'ETRE PISTE

Certains navigateurs proposent **une option pour indiquer aux sites Internet que vous refusez que l'on utilise des informations liées à votre navigation sur Internet**. Les sites commerciaux utilisent très souvent ces données pour vous proposer des offres commerciales.

Selon le navigateur que vous utilisez, le processus pour activer cette option ne sera pas le même.

Si vous utilisez Mozilla Firefox : rendez-vous dans les options, puis dans l'onglet « Vie Privée ». Cochez ensuite la case "Indiquer aux sites que je ne souhaite pas être pisté". Décochez également la case "accepter les cookies" et cochez "vider l'historique à la fermeture de Firefox".

Avec Google Chrome : dans les paramètres, rendez-vous dans la rubrique "Vie Privée", puis cochez la case "indiquer aux sites que je ne souhaite pas être pisté" et cliquez sur "OK".

Microsoft Edge : dans les Options (via l'icône « … » en haut à droite), cliquez sur "Afficher les paramètres avancés" puis activer "Envoyer des demandes Do Not Track".

Si vous utilisez encore Internet Explorer : dans l'onglet "Sécurité" du menu, cliquez sur "activer la protection contre le tracking" puis sur "activer les demandes Do Not Track".

SUPPRIMEZ REGULIEREMENT VOS DONNEES DE NAVIGATION

Si vous ne souhaitez pas activer le mode "privé" ou "incognito" de votre navigateur, nous vous recommandons toutefois de supprimer régulièrement les cookies, les fichiers temporaires ainsi que votre historique de navigation manuellement :

- **Vous utilisez Mozilla Firefox** : pour supprimer les cookies, l'historique de navigation ou les fichiers de navigation, cliquez sur "Historique" puis sur "Effacer l'historique récent". Choisissez "Cookies", "Cache" et "Historique de navigation et des téléchargements" puis supprimez-les.

- **Vous utilisez Google Chrome** : cliquez sur l'icône puis sur "Plus d'outils" et "Effacer les données de navigation". En haut de la page, choisissez une période. Pour tout supprimer, sélectionnez Toutes les périodes. Cochez les cases face à « Cookies et données de site » et « Images et fichiers en cache ». Cliquez sur "Effacer les données".

- **Vous utilisez Microsoft Edge** : Dans le navigateur Microsoft Edge, cliquez sur le bouton " … " en haut à droite. Cliquez sur Paramètres ; Dans Effacer les données de navigation, sélectionnez Choisir les éléments à effacer. Cochez la case Cookies et données de sites web enregistrées puis sélectionnez Effacer.

- **Vous utilisez Safari** : choisissez Safari, puis Préférences, cliquez sur Confidentialité, puis cliquez sur Gérer les données du site web, sélectionnez un ou plusieurs sites web, puis cliquez sur Supprimer ou Tout effacer.

- (Sur iPhone, iPad ou iPod touch : Pour effacer votre historique et vos cookies, accédez à Réglages > Safari, puis cliquez sur Effacer historique, données de site.)

- **Vous utilisez encore Internet Explorer** : sélectionnez le bouton "Outils", pointez sur "Sécurité", puis sélectionnez "Supprimer l'historique de navigation". Cochez la case "Cookies et données de sites web", puis cliquez sur "Supprimer".

NAVIGUER SUR INTERNET : INSTALLEZ UN BLOQUEUR DE PUBLICITES

Les publicités, quel que soit leur format et le site sur lequel elles se trouvent, peuvent **cacher des arnaques ou des virus potentiels.**

Les ignorer permet d'éviter ce type de souci. Pour masquer ces publicités, qui gênent d'ailleurs souvent la navigation sur vos sites web, **téléchargez un bloqueur de publicités efficace**.

Certains sites vous demanderont parfois de désactiver ce bloqueur de publicités afin de consulter leur contenu. C'est notamment le cas de certains sites de médias en ligne. Faites alors preuve de discernement, et réactivez-le dès que vous avez fini de consulter les pages en question.

FAITES ATTENTION AUX EXTENSIONS DE NAVIGATEUR QUE VOUS INSTALLEZ

Pour naviguer sur internet en toute sécurité, n'installez des extensions de navigateur ou plugins qu'en cas de besoin. Nous vous recommandons de les installer auprès des magasins officiels d'extensions de votre navigateur (Chrome Web Store, Firefox Add-ons, Microsoft Store, Safari Extensions).

NAVIGUER SUR INTERNET EN TOUTE SECURITE : FAITES PREUVE DE VIGILANCE

Même sur les sites auxquels vous êtes habitué, ou lors d'échanges avec des gens que vous connaissez, soyez toujours vigilant à ce qui vous est présenté, et à ce que vous faites.

Évitez par exemple de vous rendre sur des sites douteux, ou aux pratiques illégales. Ceux-ci sont bien souvent truffés de virus et de logiciels malveillants.

Une autre bonne pratique consiste à **vérifier l'adresse qui se trouve derrière un lien avant de cliquer dessus**. Pour ce faire, faites passer le pointeur de votre souris sur le lien sans cliquer : vous verrez l'adresse du site Internet apparaître en bas de votre page de navigation. La fin de cette adresse doit toujours être strictement identique au nom de la marque attendue. Par ailleurs, vérifiez que l'adresse du site Internet commence par "https://".

De même, évitez de vous connecter à partir d'un ordinateur ou sur un réseau Wifi publics car ils peuvent être contrôlés ou piégés par un cybercriminel. Si vous y êtes contraints, n'échangez jamais de données confidentielles (identifiant, mot de passe, numéro de carte bancaire…).

LES BONNES PRATIQUES POUR NAVIGUER SUR INTERNET : LIMITEZ LES DONNEES QUE VOUS PARTAGEZ

Lorsque vous vous inscrivez sur un site web, vous transmettez des données. Or, celles-ci peuvent être utilisées, soit par des entreprises pour vous adresser des publicités non-sollicitées, soit par des personnes malveillantes si le site a été piraté. Lorsque vous vous inscrivez sur un site web, veillez donc à **ne remplir que les champs obligatoires des formulaires**. Ils sont souvent marqués par un astérisque (*).

Sur les sites marchands, redoublez de vigilance. Consultez notre dossier dédié aux bonnes pratiques à acquérir pour naviguer sur les sites e-commerce.

Sur les réseaux sociaux, les forums ou les blogs**, ne partagez pas d'informations trop privées**. Pour ce faire, vous pouvez vous choisir un pseudonyme que vous utiliserez en ligne pour masquer votre réelle identité, ainsi qu'une adresse email qui ne permette pas de vous identifier facilement.

En appliquant ces 8 bonnes pratiques, vous éviterez de nombreux problèmes liés à la navigation sur Internet : hameçonnage (phishing), virus, piratage de compte… Si vous pensez avoir été victime de l'une de ces malveillances, vous pouvez obtenir tous nos conseils et l'accompagnement par l'un de nos professionnels en sécurité informatique référencés.