Les bonnes pratiques pour naviguer sur Internet

Pour naviguer en toute tranquillité

Penser aux informations que vous divulguez

CCAS Portiragnes

Portiragnes Mer & nature

1. Ayez toujours un navigateur à 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 sont pas mis à jour.
- 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.

2. Naviguez spontanément en mode “privé”

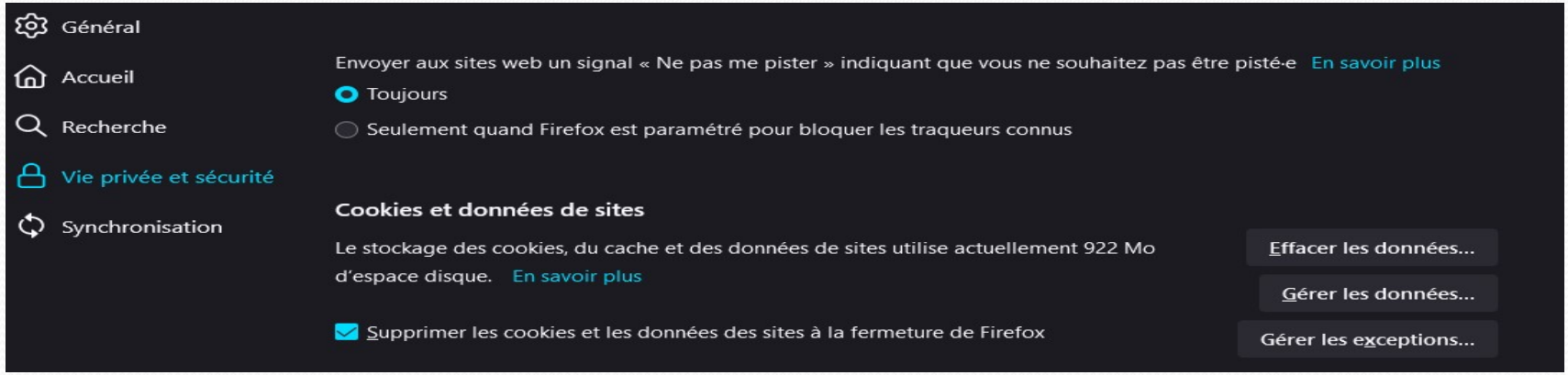
- Tous les navigateurs web possèdent un mode “incognito” ou “privé”. Son principal intérêt consiste à ne pas enregistrer l’historique de navigation sur votre appareil. Le deuxième intérêt est de limiter l’envoi d’informations aux sites Internet sur lesquels vous naviguez.
- Notez également naviguer sur 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'être pisté

- **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".

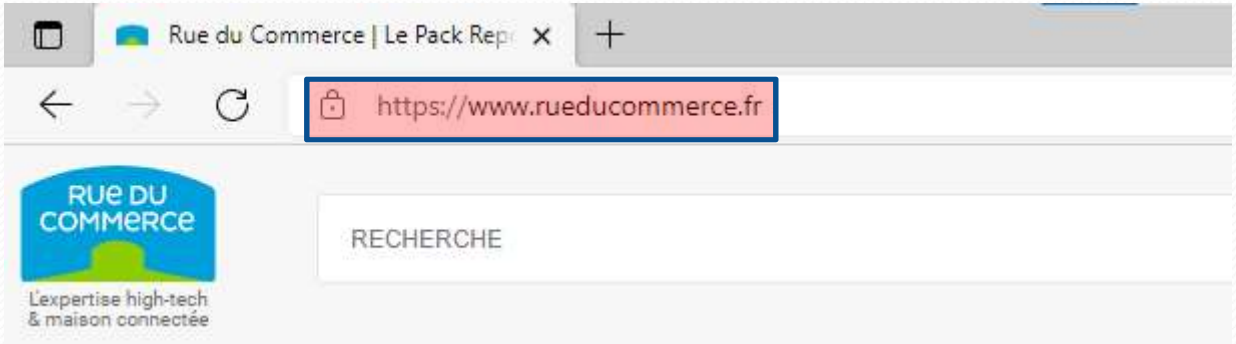
3. Configurez votre navigateur pour indiquer que vous refusez d'être pisté

- 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 et sécurité ». Cochez ensuite la case "Ne pas me 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 "Confidentialité et sécurité", puis activez la case "Interdire le suivi" et cliquez sur "OK".
- **Microsoft Edge** : dans les Options (via l'icône « ... » en haut à droite), cliquez sur.



4. Privilégiez les sites sécurisés

- Pour vérifier qu'un site est sécurisé, c'est très simple. Il suffit de regarder dans la barre de votre navigateur contenant l'URL. Si l'adresse du site commence par « https » et/ou que vous voyez un cadenas, le site est sécurisé. Le « s » de https signifie qu'il utilise un cryptage SSL, qui assure la sécurité des données que vous renseignez. Vous pouvez donc renseigner vos informations personnelles telles qu'un identifiant et un mot de passe de connexion ou des coordonnées bancaires. Cette vérification est impérative avant tout achat en ligne notamment.

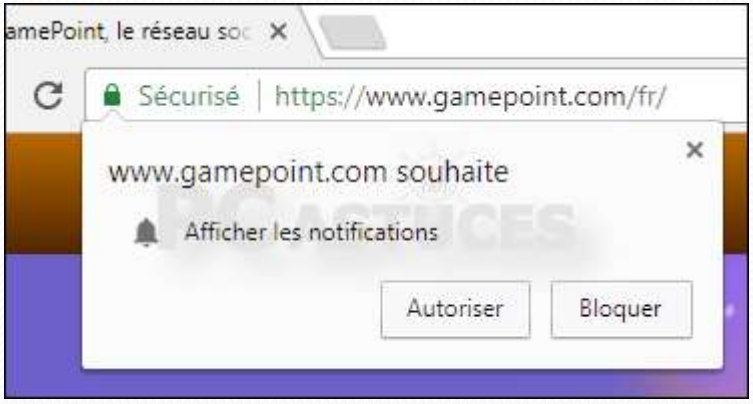


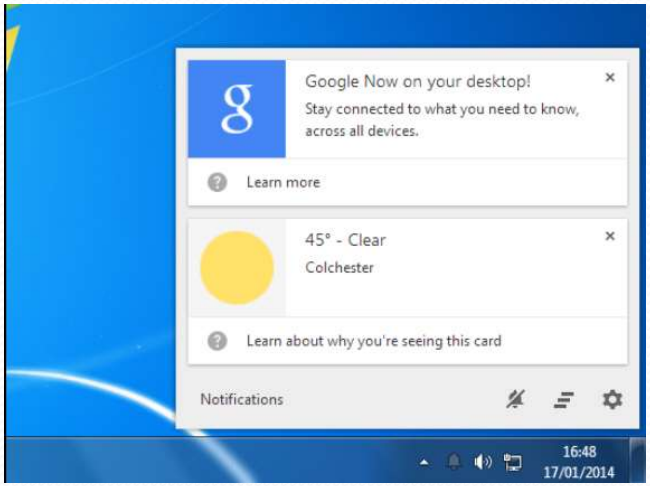
5. Évitez les réseaux wifi dit « publics »

- Qui dit public, dit facilement accessible par tous, y compris des hackers ou des pirates. Les ordinateurs ainsi que les réseaux wifi publics ou accessibles sans mot de passe sont à éviter dans la mesure du possible. Si vous y êtes contraint, alors pendant votre temps de navigation dessus, ne renseignez aucune donnée confidentielle (identifiant, mot de passe ou numéro de carte bancaire).
- Préférez le partage de connexion depuis votre Smartphone.

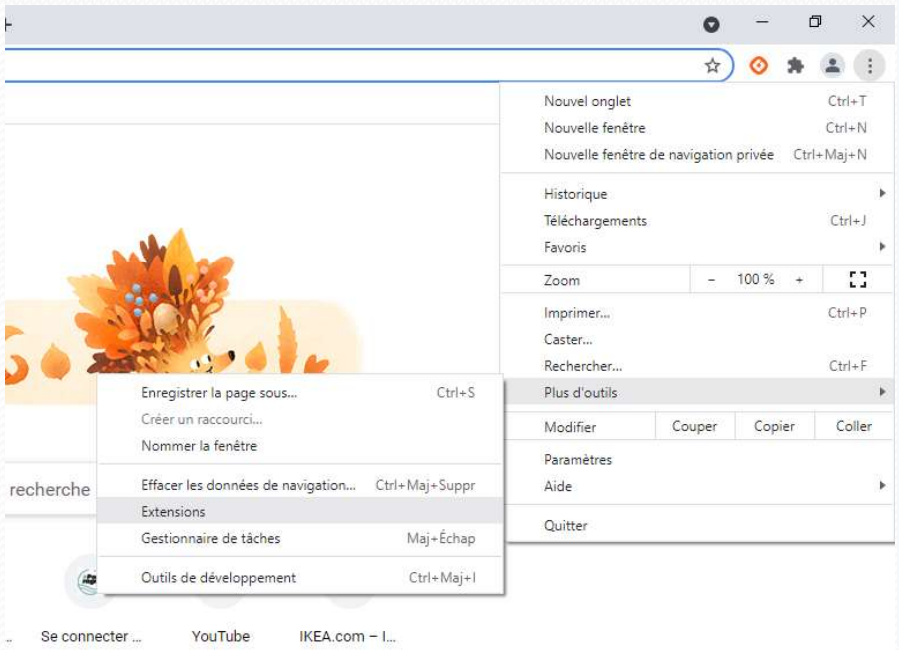
6. Faites attention aux extensions de navigateur que vous installez

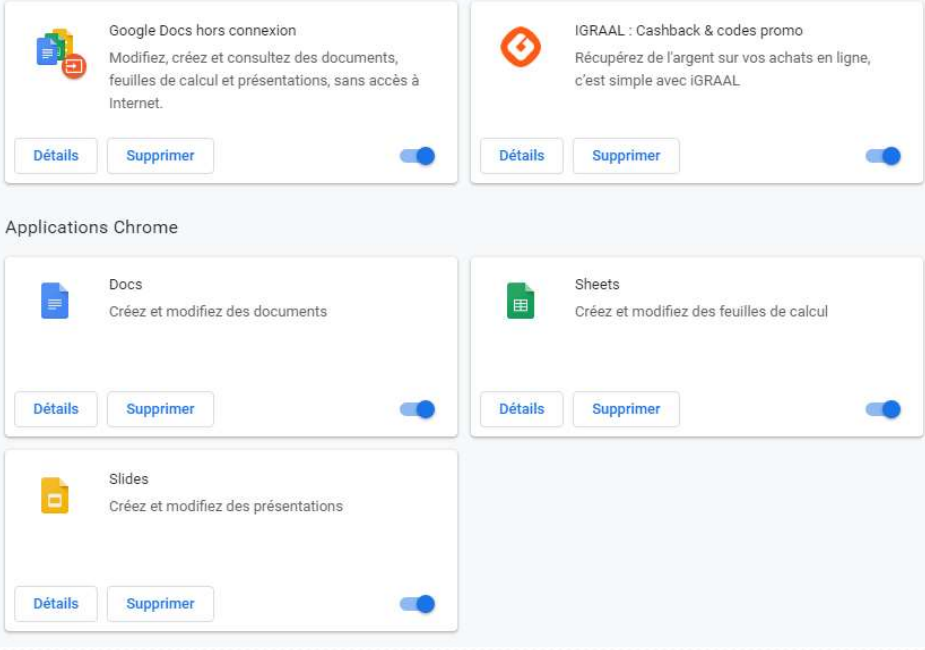
- Pour naviguer sur internet en toute sécurité, n'installez des extensions de navigateur ou plugins qu'en cas de besoin. Nous vous recommandons de les installer auprès des magasins officiels d'extensions de votre navigateur (Chrome Web Store, Firefox Add-ons, Microsoft Store, Safari Extensions).





Magasin d’extension Google Chrome





7. Limitez les données que vous partagez

- Sur internet, il n'existe pas de bouton pour supprimer totalement un contenu. Par exemple, sur les réseaux sociaux, chaque commentaire et image postés peuvent rester en ligne pour toujours. En effet, vous pouvez supprimer la publication originale mais pas les éventuelles copies faites par d'autres. Configurez les paramètres de confidentialités sur les réseaux sociaux pour que vos publications ne soient accessibles qu'à votre « réseau » et non ouvertes à tous.

Configuration Facebook

Découvrez 5 bonnes pratiques essentielles pour éviter les arnaques et escroqueries.

1. Méfiez-vous des offres trop alléchantes en terme de prix

- Il n'est pas rare d'être attiré par des prix particulièrement bas sur Internet. C'est malheureusement parfois le point de départ d'escroquerie. Avant même de penser à acheter votre produit, pensez donc à **comparer son prix sur différents sites web**.

Tirage au sort

2. Comment sécuriser ses achats sur internet : Vérifiez en amont l'autorité du site web

- Sur un site e-commerce que vous ne connaissez pas, il est recommandé de **taper dans un moteur de recherche le nom du site vendeur, suivi du mot "arnaque" ou "escroquerie"**. Vous tomberez alors sur des sites où des particuliers auront peut-être déjà signalé des tentatives d'escroquerie ou d'arnaque.
- Rechercher un numéro de téléphone, adresse postale sur le site internet.

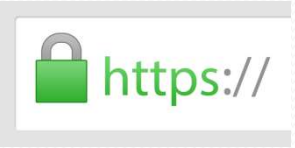
4. Comment sécuriser ses achats sur internet : Menez quelques vérifications de base au moment de payer

- Tout d'abord, sachez que **le consentement de paiement en ligne se fait, légalement, par deux clics.**
- **1. Le premier clic :**

Vous arrivez sur une page de vérification de la commande, dans laquelle les produits demandés, leur quantité, leur prix, le mode de livraison, et d'autres éléments clés seront rappelés. Vérifiez attentivement toutes ces informations et faites également attention à ce que d'autres options supplémentaires, que vous ne désirez pas, n'aient pas été rajoutées automatiquement (assurances, livraison payante…).

- **2. Le second clic confirmera effectivement la commande**

Pour le paiement, procédez à deux vérifications de sécurité : la première consiste à vérifier que l'adresse web (URL) du site comporte impérativement **la mention "https://" et non "http://"**. Le -s à la fin est symbole de sécurité : il s'agit du protocole TLS, qui garantit le chiffrement de vos données bancaires entre votre machine et le site marchand. L'idée est bien d'éviter le piratage de votre carte bancaire. Vérifiez également l'affichage, près de l'URL, d'**un pictogramme en forme de cadenas** : voilà un signe de sécurité de paiement en ligne.



5. Privilégiez les moyens de paiement les plus sécurisés

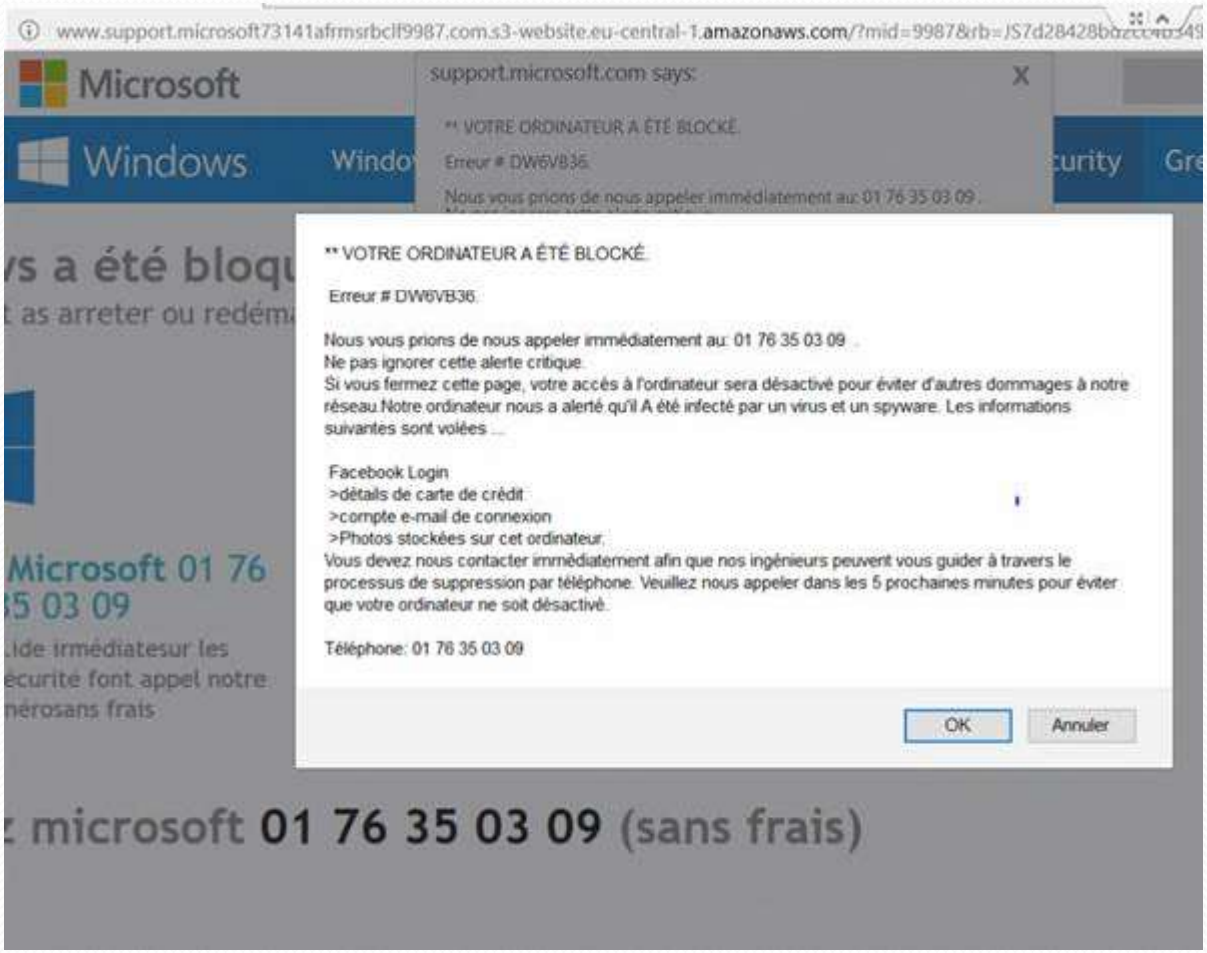
- Pour véritablement vous assurer d'éviter toute fraude, vous pouvez privilégier **les moyens de paiement en ligne type Paylib ou e-Carte Bleue.** Ils vous évitent de communiquer vos informations bancaires au vendeur et vous proposent, dans certains cas, des remboursements ou des annulations de débit si vous rencontrez un litige.
- **Si vous utilisez votre carte bancaire**, on ne doit jamais vous demander plus que quatre éléments, à savoir : votre numéro de carte, le nom associé au compte bancaire, la date de validité de la carte et le cryptogramme à trois chiffres situé au dos de la carte. Ne communiquez en aucun cas le code PIN, qui vous sert à retirer de l'argent au distributeur ou à payer avec votre carte.
- **Si vous n'allez pas régulièrement sur ce site, supprimez votre numéro de carte bancaire** sur votre compte pour qu'il ne tombe pas un jour dans de mauvaises mains.

En résumé

- En suivant ces recommandations, vous renforcerez la sécurité de votre navigation et la protection de vos données personnelles. Cependant, **en cas d'incident**, de comportement inhabituel de votre machine tel que la création, la modification ou la suppression de fichiers sans votre autorisation… Ne cédez pas à la panique et ayez les bons réflexes : **commencez par déconnecter votre ordinateur d'internet**. Vous couperez ainsi la communication entre le pirate et votre machine. Faites, si possible, une sauvegarde de vos fichiers importants (documents, photos, etc.) sur un disque dur ou une clé USB. Enfin, si votre antivirus ne parvient pas à réparer le problème, la meilleure solution est de réinstaller complètement le système d'exploitation à partir d'une version saine. N'hésitez pas à faire appel à votre prestataire informatique pour cela.

En cas de doute débrancher votre BOX internet !!!
Ne jamais donner son numéro de carte bleue, si on vous le demande

Ne jamais donner son numéro de carte bleue, si on vous le demande et que vous n'êtes pas sur le point de faire un achat !!!



Ne pas appeler ce type de numéro, lorsque vous êtes sur internet, et que ce type de fenêtre surgit.

- 1 Eteindre votre ordinateur
- 2 Débrancher votre Box

- Redémarrer votre ordinateur il y a de forte chance qu'elle n'apparaisse plus.
- Rebrancher votre Box

Montant du préjudice
En moyenne 300€

LEXIQUE

- Voici un site internet qui récence les principaux termes informatiques :
- https://www.bml49.fr/medias/files/lexique-informatique.pdf