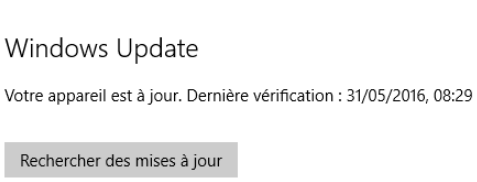
GUIDE SECURITE INFORMATIQUE



Commencez par faire les mises à jour de l'ordinateur régulièrement (système, pilotes & logiciels) pour combler les failles de Sécurité, en plus de pouvoir bénéficier éventuellement de nouvelles fonctionnalités.

N'hésitez pas à vérifier l'authenticité d'un **message suspect** auprès de l'expéditeur via un autre canal (Téléphone, SMS …) avant d'ouvrir une pièce jointe (en particulier les fichiers de type fausses factures, faux actes notariés, … ou .exe qui sont en fait des applications) ou de cliquer sur un lien dans le message (il vaut mieux faire une recherche du site directement dans votre moteur de recherche). Vérifiez que la liste des destinataires n'est pas suspecte à vos yeux. Faîtes particulièrement attention aux messages écrits en anglais ou mal traduits. En cas de doute, supprimez le message sans le transférer.

Eviter de faire suivre les « chaines » afin de ne pas diffuser votre adresse inutilement. Les conséquences sont multiples : encombrement des réseaux, désinformation… Vous devenez des vecteurs publicitaires et surtout les données personnelles sont ainsi divulguées à des tiers.

Si vous avez besoin de faire un envoi à plusieurs contacts qui ne se connaissent pas, **privilégiez le champ CCI**

Tenez à jour votre carnet d'adresses en **supprimant les contacts obsolètes** régulièrement. En cas de piratage de votre messagerie, cela réduit la propagation des menaces existantes.

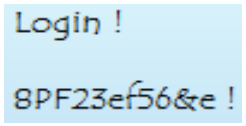
N'utilisez que des **moteurs de recherche** connus et fiables tels qu'Exalead (français), Qwant (validé pour les enfants), Google, Bing, …

De même, faîtes **attention à la provenance des clés USB** que vous connectez à vos ordinateurs.

N'installez que des logiciels utiles, téléchargés à partir des sites officiels (http://offurl.fr/ peut vous guider), tout en faisant attention à décocher toute demande d'ajout de logiciels tiers et/ou toolbar qui sont sélectionnés par défaut.
Ces dernières peuvent automatiquement remplacer votre moteur de recherche défini par défaut.

Evitez aussi l'usage des assistants vocaux intégrés qui augmentent sensiblement la surface d'attaque

Limitez les inscriptions sur des sites Internet et sécurisez vos mots de passe (8 caractères minimum dont au moins une majuscule, minuscules, chiffres & caractères spéciaux). Aussi, il est important de procéder fréquemment à son changement (tous les 6 mois environ) et d'en avoir un différent par site. Ne les écrivez pas sur un autre support qu'un coffre d'identifiants sécurisés.



Faîtes **attention aux données diffusées** sur internet, notamment sur les réseaux sociaux (Facebook, Twitter, et tous les autres...) ainsi que les nuages (Cloud).

Faîtes régulièrement une **sauvegarde** de vos fichiers importants.

Lors de vos échanges sur internet (réseaux sociaux, tchat, messagerie…) **ne divulguez pas à un inconnu vos habitudes** (départ de vacances, critères physiques surtout pour les mineurs …) afin d'éviter les attaques personnelles, cambriolages…

Il est **déconseillé de faire retenir les identifiants** par le navigateur ou une application contenant des données sensibles, surtout si vous utilisez un Ordinateur partagé (Cybercafé, …) ou un terminal mobile.

- Dans ce dernier cas, privilégiez le **partage de connexion sur un téléphone mobile** de confiance plutôt que de vous connecter à un réseau Wifi (HotSpot, Connexion Publique, Hôtel, Restaurant, …).

- **Désactivez systématiquement le WiFi et le BlueTooth** de vos appareils quand vous n'en avez pas besoin.

- **Changez systématiquement les codes de déverrouillage** par défaut sur vos téléphones, tablettes, … et **privilégiez le déverrouillage par reconnaissance faciale ou de l'empreinte digitale**.

Sur votre Ordinateur, **verrouillez votre session avec Windows+L** lorsque vous devez vous absenter.

- **Assurez-vous que le site est certifié «** 

» avant de mettre en ligne des données sensibles, et effectuer des achats en ligne. Dans ce dernier cas, **vérifiez l'identité du vendeur, de préférence Français ou Européen** si vous avez besoin d'un recours**, et sa e-réputation** avec une recherche sur Internet associée au mot « arnaque ».

- Prenez le temps de **bien lire les messages d'avertissements** des systèmes, applications, sites internet, … avant d'exécuter un programme ou d'ouvrir un fichier. Ne prenez pas de risques si vous avez un doute.

- Si vous n'utilisez pas les fonctionnalités avancées de vos **logiciels Adobe, désactivez Javascript :** https://helpx.adobe.com/fr/acrobat/11/using/javascripts-pdfs-security-risk.html

- **En cas d'infection ou attaque, déconnectez votre matériel** du WiFi ou du réseau et ne l'éteignez pas tant qu'il n'aura pas été étudié par un professionnel. N'appelez surtout pas le numéro d'un support qui apparaîtrait à l'écran, il s'agit probablement d'une arnaque. Prenez votre écran en photo pour le dépôt de plainte. Privilégiez enfin votre professionnel habituel pour le rétablissement de votre ordinateur.

Annexes

- Le site https://www.cybermalveillance.gouv.fr/ vous délivre nombre de bonnes pratiques

- Un second site officiel permet de se former progressivement jusqu'en Avril 2020 : https://secnumacademie.gouv.fr/

- Le Ministère de l'Intérieur a mis en place une **plateforme d'information** afin de sensibiliser et protéger les internautes.

- Le Ministère de la Défense recrute des Combattants numériques **volontaires pour la cyberdéfense informatique**. Plus d'information sur ce **lien** .

- Dans le cadre du **plan d'action contre la radicalisation et le terrorisme** du Ministère de l'Intérieur, il est demandé d'être particulièrement vigilant sur tous contenus visant le recrutement et la propagande (contenu vidéo Youtube, pages réseaux sociaux, …)