Résumé Atelier
Sécurité informatique

L'ordinateur

Dans une majorité de cas, Windows 10 gère très bien lui même la sécurité de l'ordinateur :

Vous n'avez rien à faire.

Windows 10 dispose d'un système de sécurité **très performant** si il est **mis à jour**, vérifiez donc qu'elles soient faites **au plus vite**.

La sécurité dans un usage **quotidien et normal** d'un ordinateur ne représente **aucun risque**. Pour qu'un fichier représente une menace, il doit avoir été ajouté dans l'ordinateur en passant à travers **différents filtres** :

- La sécurité du service de messagerie / service de téléchargement
- La sécurité du navigateur (A noter que Google Chrome dispose d'un antimalware intégré permettant l'analyse des fichiers)
- L'antivirus de Windows 10

Les chances d'être infectés, bien qu'existantes, sont **très faibles**.

Les sites les plus «dangereux» sont généralement ceux qui permettent de télécharger **illégalement** des fichiers, souvent des logiciels à la base payants.

Il convient aussi d'adopter plusieurs réflexes afin de minimiser les chances d'être infecté :

- Ne **jamais** télécharger un fichier **exécutable** provenant d'un **mail**
- Plus généralement, **éviter** de télécharger les fichiers dont vous ne connaissez pas la **source**
- **Toujours** aller sur le site de l'éditeur pour **télécharger un logiciel** (et éviter de passer par **Clubic** ou **01net**, par exemple, qui ajoutent souvent un logiciel **sponsorisé** dans l'exécutable)

Contact en cas de besoin:
espacetechnoal@gmail.com ou ***damien.duez@conseiller-numerique.fr***

La navigation sur Internet

Le sujet étant vaste, il convient de préciser que le sujet n'est abordé qu'en surface.

Voici plusieurs pratiques et réflexes à mettre en place :

Vérifier la cohérence d'un lien : Passer sa souris sur un lien (sans cliquer), permet au navigateur d'afficher l'adresse cible en bas à gauche de la fenêtre. Si les deux liens ne correspondent pas, il s'agit très certainement d'une arnaque.

Dans les mails : Vérifier toujours l'expéditeur, en cas de doute : https://www.nom-domaine.fr/whois.html

Vérifier l'orthographe (attention, des coquilles ça arrive à tout le monde, on parle d'un nombre de fautes anormal pour une institution).

Une institution n'utilise jamais des services accessibles à tout le monde pour ses propres mails : si les impôts vous réclament de l'argent avec une adresse @Gmail.com ou @hotmail.fr, c'est forcément une fraude.

Impossible qu'une institution de l'état envois un mail pour exiger un paiement, plus spécifiquement impossible en passant par paypal/western union ou autre moyen de paiement douteux à base de cartes prépayées

Mettre un mot de passe complexe, avec au moins une majuscule, un chiffre et un caractère spécial : motdepasse, 123456 ou la date de naissance : c'est non

Le cadenas ou S de HTTPS :

Il s'agit d'un chiffrement des données, les rendant illisibles à un tiers tant que le cadenas est présent. Il est très important de vérifier que le cadenas est présent au moment où j'entre des données personnelles.

Contact en cas de besoin:
espacetechnoal@gmail.com ou ***damien.duez@conseiller-numerique.fr***