Se protéger et Protéger sa machine

Que peut-on craindre ?

- La perte de données suite à une défaillance matérielle ou humaine.
- L'indiscrétion ou l'atteinte volontaire à l'intégrité des données par une personne.
- La révélation des habitudes de navigation.
- L'attaque du système par un logiciel malveillant ou un pirate.

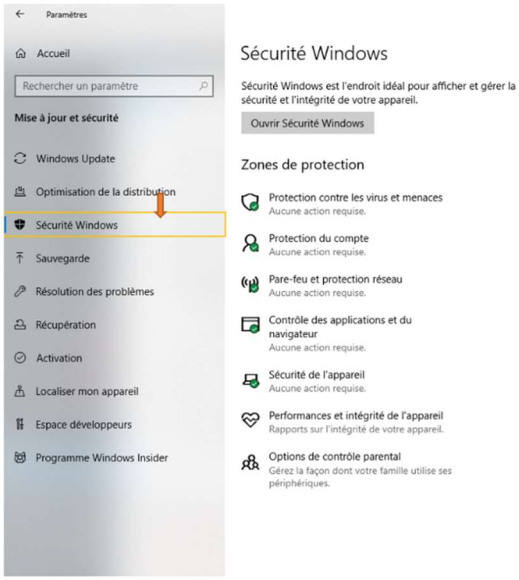
Comment sécuriser son espace de travail local et distant ?

- En sauvegardant régulièrement ses données sur des supports amovibles ou distants.
- En limitant l'accès à son espace de travail et ses fichiers, mettez un code à votre ordinateur/smartphone
- En maîtrisant ses traces.
- En protégeant son système des logiciels malveillants, la premiere défense est la vigilance, suis sûr de la source !
- En identifiant les situations à risque.
- En étant capable de restaurer l'intégrité de son système.
- En déposant ses fichiers dans un espace privé.
- En limitant tout risque d'usurpation d'identité (mot de passe complexe ; déconnexion de sa session ; etc.)

Pour sécuriser son espace de travail, il faut éviter les comportements à risques et avoir un logiciel de protection installé sur sa machine.

Pour limiter les risques, il faut être vigilant…

- Ne pas ouvrir les fichiers dont on ne connaît pas l'origine : les fichiers exécutables (d'extension exe, sys, com, jar, etc.) peuvent infecter l'ordinateur et certains fichiers de bureautique peuvent contenir des macro virus.
- Ne pas croire qu'un fichier envoyé par un ami provient forcément de lui. Son système a pu être contaminé par un logiciel malveillant ou on a pu usurper son identité.
- Ne pas installer sur l'ordinateur des logiciels dont on ne connaît pas l'origine. Préférer les sites officiels ou reconnus pour télécharger une application.
- Mettre à jour régulièrement le système d'exploitation et les logiciels pour apporter des correctifs aux failles corrigées.



... et installer un logiciel de protection sur sa machine.

Windows à par défaut un antivirus installé qui fonctionne très bien.

Quand un virus infecte un fichier, il place dans celui-ci un code spécifique : c'est la **signature virale**.

Un **antivirus** est un logiciel conçu pour protéger les ordinateurs des logiciels malveillants (virus, ver, cheval de Troie ou logiciel espion). Il

possède une base de données de signatures virales et scanne les fichiers à la recherche de ces signatures dans leur code.

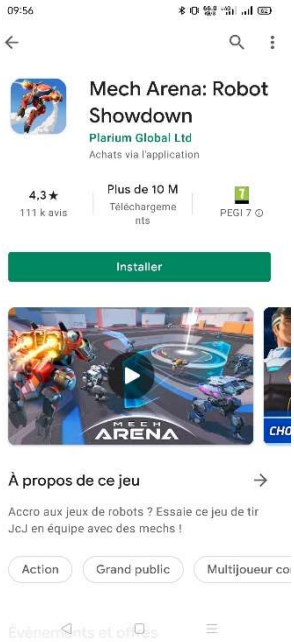
Un antivirus a trois principales fonctionnalités :

- une **protection résidente** ou veille, qui analyse tout nouveau fichier entrant ;
- un **scanner** qui peut analyser un support et y rechercher les logiciels malveillants ;
- un module de **mise à jour** (automatique) des signatures virales. S'il détecte un fichier infecté, il offre plusieurs possibilités :
- il tente de le réparer en éliminant le virus ; • il le place en quarantaine en l'empêchant d'agir :
- il supprime le fichier contaminé.

Un **pare-feu** ou *firewall* est un système permettant de protéger l'ordinateur des intrusions extérieures par le réseau. Il agit comme un filtre entre le réseau et l'ordinateur.

Le pare-feu a pour but de protéger les données sensibles (mots de passe, identités, données personnelles, etc.) contre les attaques de pirates qui cherchent à les dérober ou à installer des logiciels pouvant prendre le contrôle de l'ordinateur.

Pour y accéder, Paramètre > Mise à jour et sécurité > puis Sécurité Windows.



Tout est automatiquement activé, mais vous pouvez installer un autre antivirus si vous le souhaitez : Norton, AVG, Eset etc.

Android est trés sécurisé, mais il faut tout de même rester vigilant et ne pas installer n'importe quoi.

Quand on installe une application, on vérifie quelle soit sécurisée, on se fit au mieux à sa réputation, on fait défiler et on regarde 2-3 trucs important :

- L'éditeur, si on le connait
- Le nombre de téléchargement
- La note des avis
- Et on lit les avis, souvent il y aura écrit par des utilisateurs des indications si c'est une application contenant des malware ou non

Et si l'application ne parait pas de confiance j'en télécharge une autre.

Distinguer les logiciels malveillant

Un **logiciel malveillant** ou *malware* est un logiciel développé par un pirate dans le but de nuire à un système informatique.

Il existe différents types de logiciels malveillants.

*« Un **virus** est un logiciel malveillant, généralement de petite taille, qui se transmet par les réseaux ou les supports d'information amovibles, s'implante au sein des programmes en les parasitant, se duplique à l'insu des utilisateurs et produit ses effets dommageables quand le programme infecté est exécuté ou quand survient un évènement donné. » sur FranceTerme*

On distingue :

- le **virus de boot** : il est chargé en mémoire au démarrage et prend le contrôle de l'ordinateur ;
- le **virus d'application** : il infecte un programme exécutable et se déclenche à l'exécution de celui-ci ;
- le **macro virus** : il infecte les documents bureautiques en utilisant leur langage de programmation (le VBA d'excel) .

« Un **ver** est un logiciel malveillant indépendant qui se transmet d'ordinateur à ordinateur par l'internet ou tout autre réseau et perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs. »

Contrairement au virus, le ver ne s'implante pas au sein d'un autre programme. Il se propage de façon autonome. Les vers sont souvent conçus pour saturer les ressources disponibles ou allonger la durée des traitements. Ils peuvent aussi détruire les données d'un ordinateur, perturber le fonctionnement du réseau ou transférer frauduleusement des informations.

- Un **cheval de Troie** ou **Troyen** est un logiciel apparemment inoffensif, installé ou téléchargé et au sein duquel a été dissimulé un programme malveillant qui peut par exemple permettre la collecte frauduleuse, la falsification ou la destruction de données. Le cheval de Troie ne se reproduit pas.
- Un **logiciel espion** ou *spyware* est un logiciel destiné à collecter et à transmettre à des tiers, à l'insu de l'utilisateur, des données le concernant ou des informations relatives au système qu'il utilise.
- Un **logiciel publicitaire** ou *adware* est un logiciel qui affiche des annonces publicitaires sur l'écran d'un ordinateur et qui transmet à son éditeur des renseignements permettant d'adapter ces annonces au profil de l'utilisateur. Le logiciel publicitaire est souvent intégré ou associé à un logiciel gratuit ou à un partagiciel ayant un objet différent. Les logiciels publicitaires sont souvent assimilés à des logiciels espions.
- Le **RamsonWare**, ou **Winlock,** bloque l'ordinateur aussitôt qu'il infecte le système, il verrouille en premier lieu l'ordinateur et affiche ensuite une grande alerte déclarant que l'utilisateur doit payer une amende de 100 euros pour déverrouiller sa machine. Le plus connu est le Virus de la gendarmerie.

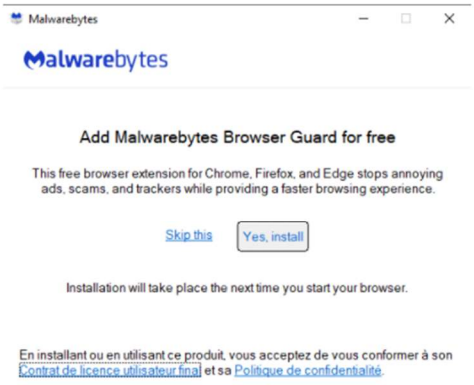
Site de confiance pour la protection **http://www.secuser.com/**

Le logiciel à utiliser en cas de problème de malware ou logiciel publicitaire Cybersécurité Malwarebytes pour les particuliers et les entreprises | Malwarebytes

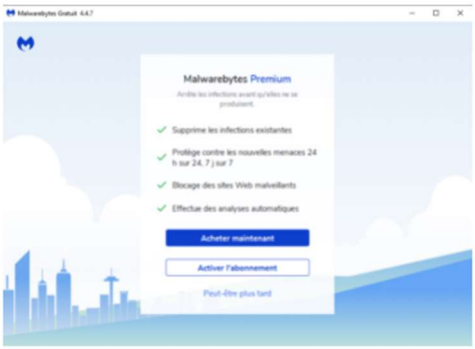
Vous télécharger le logiciel le logiciel et le lancez :

C'est un logiciel payant qui propose une version gratuite à lancer à la demande, pas besoin malgré leur sollicitation de faire autre chose, Quand vous avez fini, vous pouvez le désinstaller (ou l'acheter bien sûr)

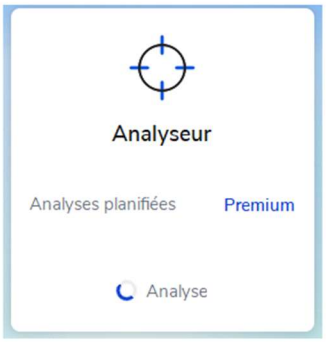
Ordinateur personnel puis Installer



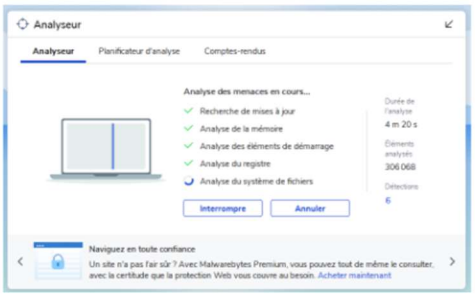
Cliquez sur "Skip This"



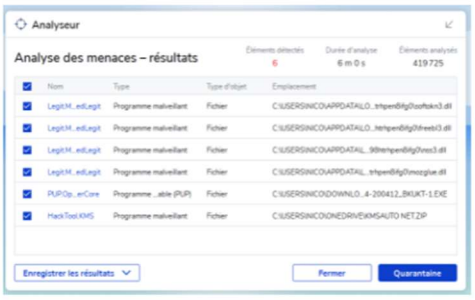
Puis "Peut-être plus tard



Puis "analyse", et laissez faire



Ca tourne



Vous cliquez sur "Quarantaine" puis "Terminer"

Plus il y a de résultats, plus vous êtes infecter, vous pouvez faire une analyse manuelle toutes les 3 ou 4 semaines si vous ne vous sentez pas sécurisé.

C'est à vous

Avez vous des problèmes récurent ?
Vous avez résolu le problème ? Comment vous avez fait ?
Qu'a fait le réparateur que vous aurez pu faire ?

Installez et lancez MalawareBytes

Ajoutez vos notes