Apprendre à sécuriser son ordinateur et sa tablette

<u>Apprenez à</u> :

- Distinguer virus, malwares et spybots et à bien vous en protéger

- Sécuriser documents et dossiers sur votre bureau

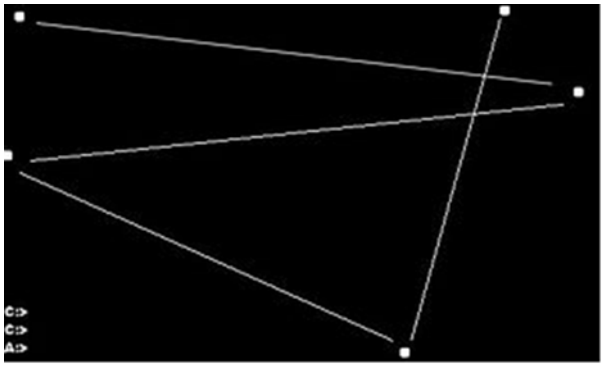
Partie 1 : Protéger son ordinateur

1. Quelques définitions

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable.

- **Un logiciel malveillant ou maliciel** (en anglais : **malware**) est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté.

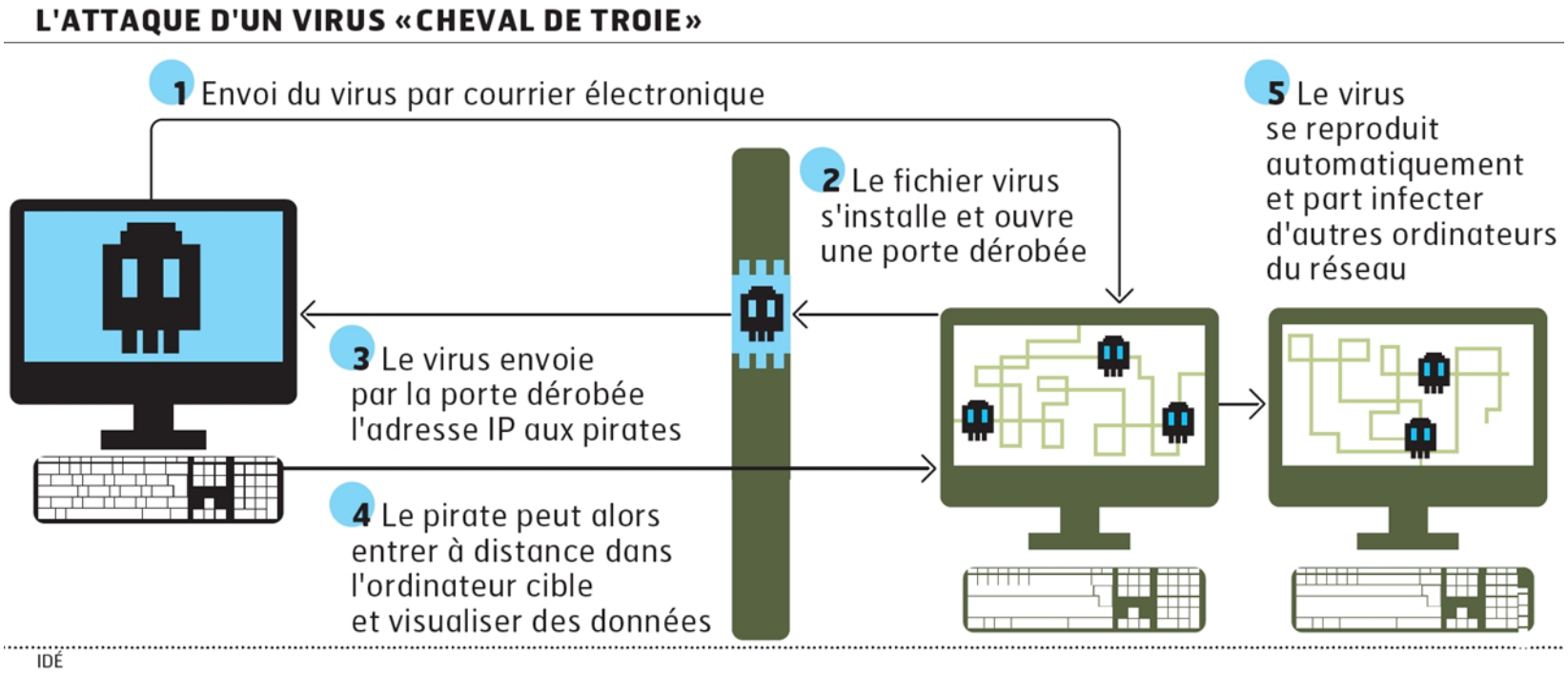
- De nos jours, le terme « **virus** » est souvent employé, à tort, pour désigner toutes sortes de logiciels malveillants. En effet, les **maliciels** englobent les virus, les vers, les chevaux de Troie, ainsi que d'autres menaces. La catégorie des virus informatiques, qui a longtemps été la plus répandue, a cédé sa place aux chevaux de Troie en 2005.



Le virus Ping-Pong, découvert le 1 mars 1988, fait rebondir de manière aléatoire une petite balle sur l'écran en bloquant tout les autres services.

- **Un virus** est un bout de code de quelques octets (pour le rendre quasi invisible à "l'œil nu") dont la fonction est destructrice ou très gênante. Son but est de détruire une partie ou toutes les données de l'ordinateur, ou encore de rendre inutilisables certaines fonctions du PC. Il peut en outre ralentir certaines procédures.

- **Le cheval de Troie** : Un cheval de Troie est un programme installé discrètement par un pirate sur votre ordinateur. Lorsque ce programme est lancé, il va causer des actions plus ou moins graves sur votre ordinateur, comme supprimer des mots de passe, voler des mots de passe, envoyer des informations confidentielles au créateur du programme, formater votre disque dur, etc.



- **Le ver** : Un ver est un petit programme qui se copie d'ordinateur en ordinateur. La différence entre un ver et un virus est que le ver ne peut pas se greffer à un autre programme et ne peut donc pas l'infecter, il va simplement se copier d'ordinateur en ordinateur par l'intermédiaire d'un réseau comme Internet ou grâce aux échanges de périphériques comme les clés USB. Le ver peut donc non seulement affecter un ordinateur, mais aussi dégrader les performances des réseaux. Comme un virus, le ver peut contenir une action nuisible qui peut être très grave comme le formatage de votre disque dur ou l'envoi de données confidentielles.

La plus célèbre anecdote à propos des vers date de 1988. Un étudiant (Robert T. Morris, de Cornell University) avait fabriqué un programme capable de se propager sur un réseau, il le lança et, 8 heures après l'avoir lâché, celui-ci avait déjà infecté plusieurs milliers d'ordinateurs. C'est ainsi que de nombreux ordinateurs sont tombés en pannes en quelques heures car le « ver » (car c'est bien d'un ver dont il
s'agissait) se reproduisait trop vite pour qu'il puisse être effacé sur le réseau. De plus, tous ces vers ont créé une saturation au niveau de la bande passante, ce qui a obligé la NSA à arrêter les connexions pendant une journée.

Voici la manière dont le ver de Morris se propageait sur le réseau :

- Le ver s'introduisait sur une machine
- il dressait une liste des machines connectées à celle-ci
- il forçait les mots de passe à partir d'une liste de mots
- il se faisait passer pour un utilisateur auprès des autres machines
- il créait un petit programme sur la machine pour pouvoir se reproduire
- il se dissimulait sur la machine infectée et ainsi de suite.

- **Le Spyware** (ou logiciel espion) : Un logiciel espion (aussi appelé **mouchard** ou **espiogiciel** ; en anglais spyware) est un logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et de transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. L'essor de ce type de logiciel est associé à celui d'Internet qui lui sert de moyen de transmission de données.

- **Phishing** (ou **hameçonnage**) : L'hameçonnage, phishing ou filoutage est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale. Elle peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques.

Lorsque cette technique utilise les SMS pour obtenir des renseignements personnels, elle s'appelle **SMiShing.**

Credit Mutuel - Adhesion (noreply@cmne.creditmutuel.fr) Ajouter aux contacts 26/11/2015

À : [redacted]

Documents via internet

Crédit Mutuel
LA banque à qui parler

Cher(e) Client(e),

vous avez été informer de l'obligation d'adhérer à la nouvelle réglementation concernant la fiabilité pour les achats par C.B. sur internet et de la mise en place d'un arret pour vos futurs achats.Or, nous n'avons pas,à ce jour,reçu d'adhésion de votre part et nous =sommes au regret de vous informer que vous pouvez plus utiliser votre cartesur internet, pour cela nous vous invitons à faire votre adhésion .

Adhésion : Faites votre demande d'adhésion en cliquant ici

Merci de la confiance que vous nous témoignez.
Cordialement,

2. Le rôle de l’antivirus

Un antivirus est un logiciel qui a pour but de détecter et d'éradiquer les virus présents dans votre PC, et de prendre des mesures pour les empêcher de nuire.

a) Les techniques de détections des virus

- **Détection de la signature**

On l'appelle aussi scan ou scanning. C'est la méthode la plus ancienne et la plus utilisée. Cette méthode consiste à analyser le disque dur à la recherche de la signature du virus, qui est présente dans la base de données du logiciel, si celui ci est à jour et si il connaît ce virus.

La signature est un morceau de code ou une chaîne de caractères du virus qui permet de l'identifier. Chaque virus a sa propre signature, qui doit être connue de l'antivirus. Cette méthode n'est pas efficace contre les nouveaux virus ou les virus dits polymorphes, dont la signature change à chaque réplication.

L'avantage de la technique du scan est qu'elle permet de détecter les virus avant leur exécution en mémoire, dès qu'ils sont stockés sur le disque et qu'une analyse est exécutée.

Pour rester efficace, l'antivirus doit procéder à la mise à jour régulière de sa base de données antivirale. Une fréquence de mise à jour mensuelle est un minimum acceptable.

- **Le contrôle d'intégrité**

Il permet de vérifier l'intégrité d'un fichier en vérifiant s'il a pas été modifié ou altéré au cours du temps. L'antivirus, va stocker un fichier central recensant l'ensemble des fichiers présents sur le disque auxquels il aura associé des informations qui peuvent changer lorsqu'il est modifié (la taille, la date et heure de dernière modification, etc.)

Lorsqu'une analyse est effectuée (ou à l'ouverture du fichier si l'antivirus réside en mémoire), l'antivirus recalcule la somme de contrôle et vérifie que les autres paramètres n'ont pas été modifiés. Si une anomalie se présente, l'utilisateur est informé.

Pour contrer en partie cette parade, les virus ne modifient pas forcément la date de modification du fichier, ou la rétablissent.

- **L'analyse heuristique**

C'est la méthode la plus puissante car elle permet de détecter d'éventuels virus inconnus par votre antivirus. Elle cherche à détecter la présence d'un virus en analysant le code d'un programme inconnu (en simulant son fonctionnement). Elle provoque parfois de fausses alertes. Par exemple : Itunes a été un temps détecté comme virus par avast.

b) Le comportement du virus

L'antivirus surveille en permanence le comportement des logiciels actifs (si il est en fonctionnement et que la protection automatique est activée). Il analyse tous les fichiers modifiés et crées. En cas d'anomalie, il avertit l'utilisateur par un message explicite. Cette protection est indispensable lorsque vous surfez sur internet.

Lorsque l'antivirus à détecté un virus, il offre trois possibilités à l'utilisateur.

- **Réparer le fichier** : L'antivirus doit être capable de réparer un fichier atteint. Mais ce n'est pas toujours possible.
- **Supprimer le fichier** : Si l'antivirus n'est pas capable de supprimer le fichier, vous pouvez le supprimer manuellement.
- **Mise en quarantaine du fichier infecté** : C'est une solution d'attente. L'antivirus place le fichier dans un dossier sûr du disque dur. Lorsque l'antivirus sera capable de réparer le fichier, vous pourrez extraire le fichier du dossier et le réparer (ne comptez pas dessus si des données sensibles sont en quarantaine).

c) Comment choisir un antivirus ?

Les logiciels gratuits ont l'avantage d'être assez légers pour ne pas ralentir les ordinateurs. **Avast, AVG** et **AVIRA** sont les champions dans cette catégorie. Leur point faible est qu'ils ne protègent l'utilisateur que des attaques les plus courantes. Cela oblige à rester très vigilant, notamment au niveau des e-mails, du streaming et des téléchargements.
Les suites payantes proposent des boucliers plus complets, pour sécuriser les transactions financières, protéger contre le vol de données personnelles et l'usurpation d'identité. **Norton**, **BitDefender** ou **Kaspersky** sont parmis les meilleurs. Ils peuvent garantir la sécurité de plusieurs ordinateurs, ainsi que des tablettes et des téléphones portables.

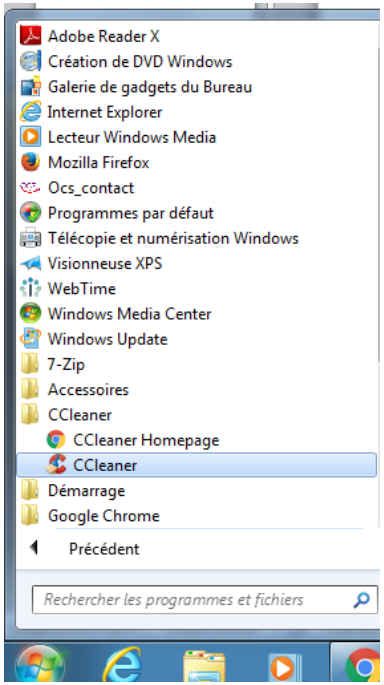
<u>Mais tout cela ne sert à rien si vous oubliez les mises à jour.</u>

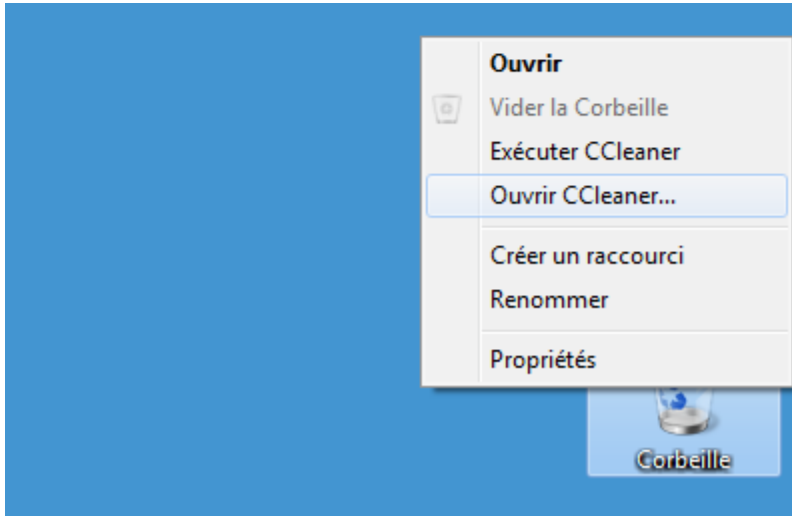
3. Comment se protéger des malwares, spywares et autres parasites (en complément d'un bon antivirus)

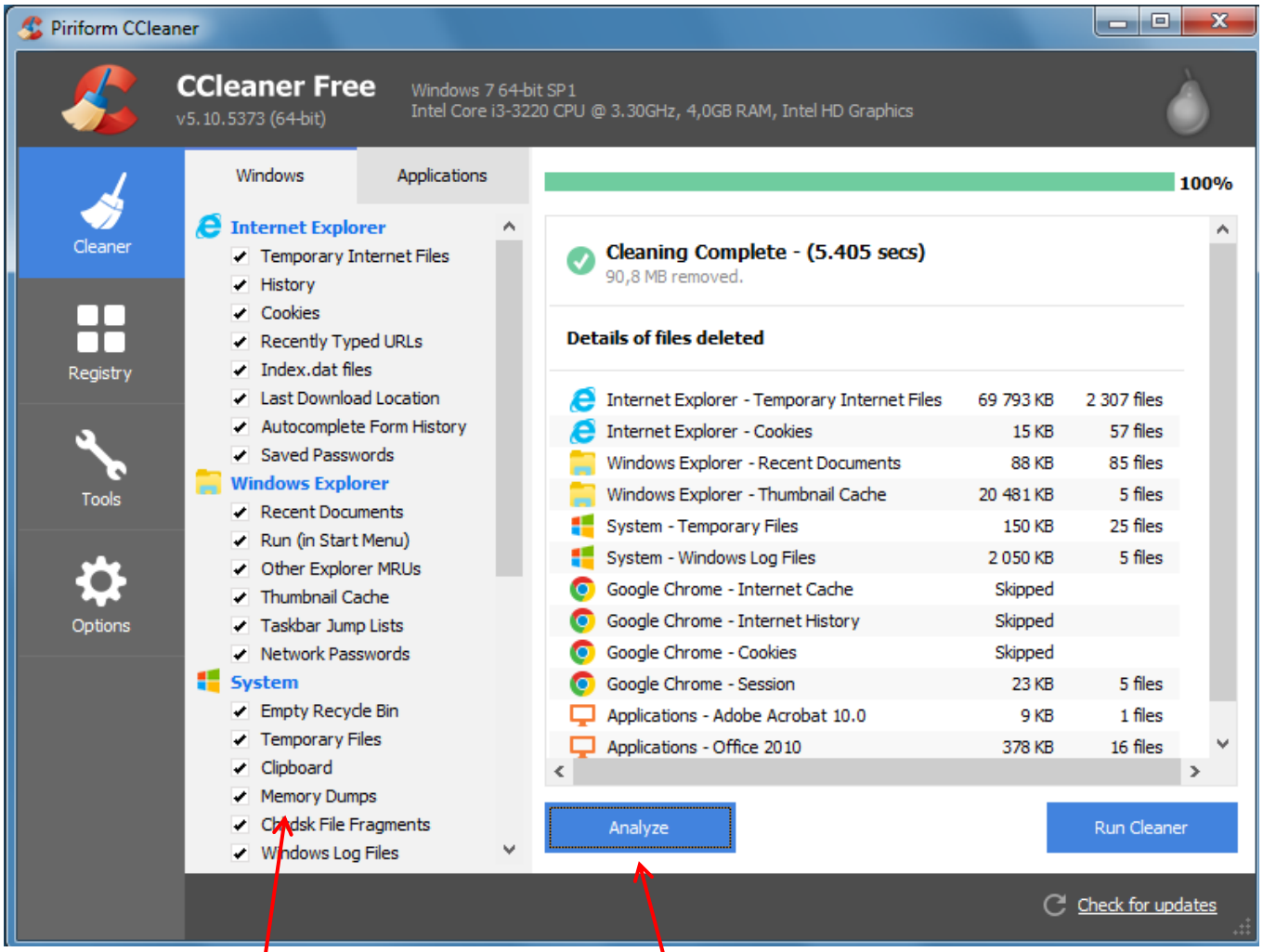
a) Ccleaner

CCleaner est un utilitaire gratuit de nettoyage pour Windows permettant de récupérer de l'espace disque disponible, tout en allégeant le fonctionnement et le démarrage du système. Entièrement gratuit, il permet de vérifier et d'optimiser le système
Adresse de téléchargement : http://ccleaner.fr/

Ccleaner s'installe comme n'importe quel logiciel. Vous double-cliquez sur le fichier téléchargé et cliquez sur « suivant » jusqu'à ce qu'il soit totalement installé.
Pour le lancer, vous pouvez aller le chercher dans vos programmes ou faire un clic droit sur la poubelle.







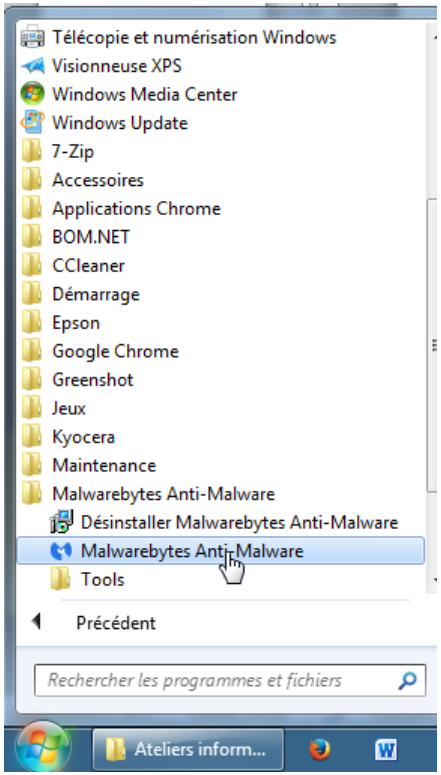
Cochez toutes les cases, puis cliquez sur « analyze ». Le processus est assez rapide (pas plus de 2min en général). Attention, cependant, rappelez-vous bien que Ccleaner videra votre corbeille.

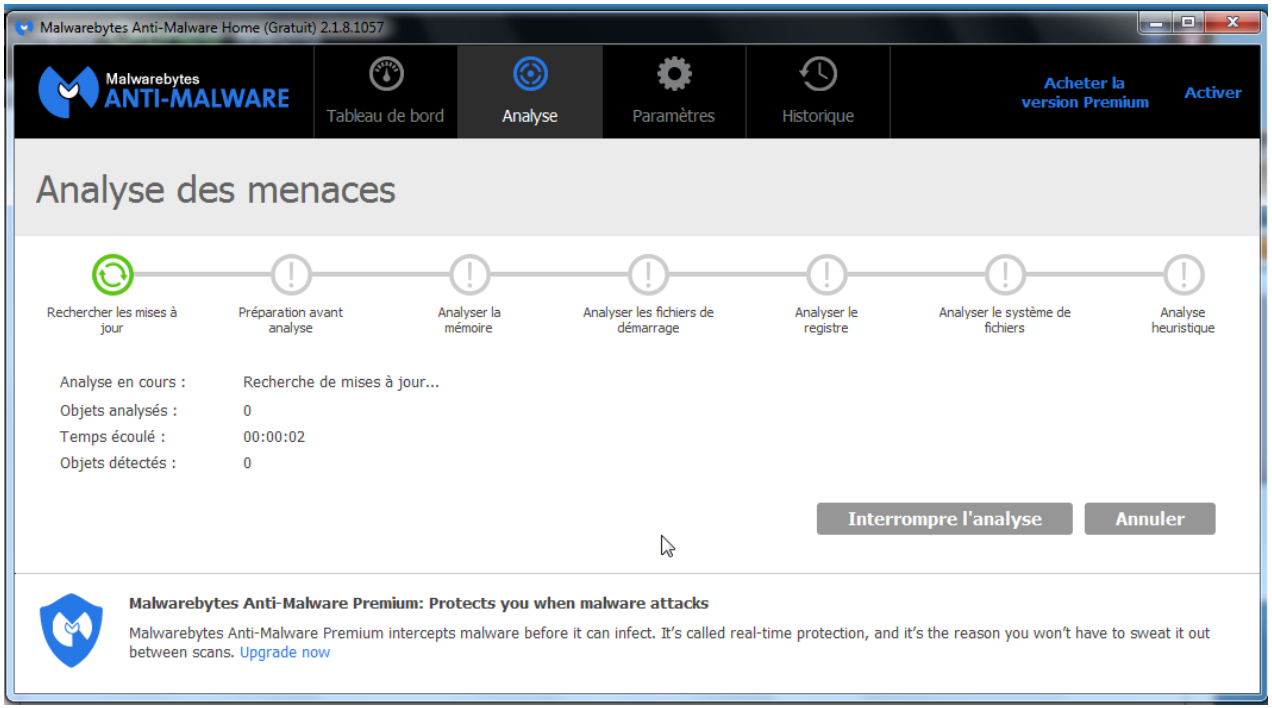
Fréquence : Tous les mois.

b) Malwarebytes

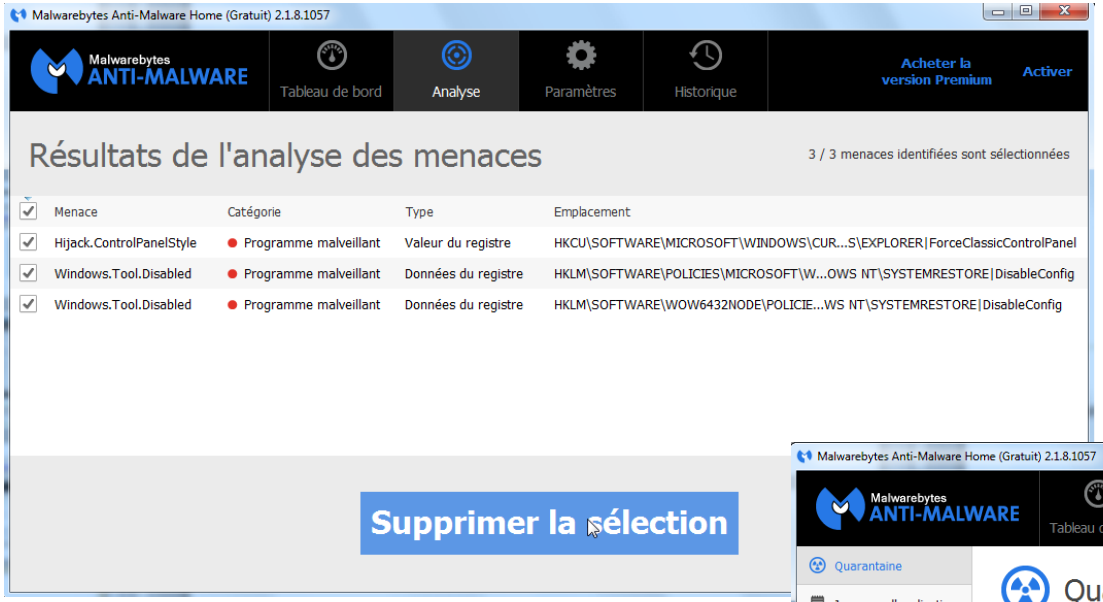
Malwarebytes Anti-Malware est un logiciel gratuit et efficace qui protège votre système contre les logiciels malveillants (spywares, malwares, etc.).
Adresse de téléchargement : https://fr.malwarebytes.org/downloads/

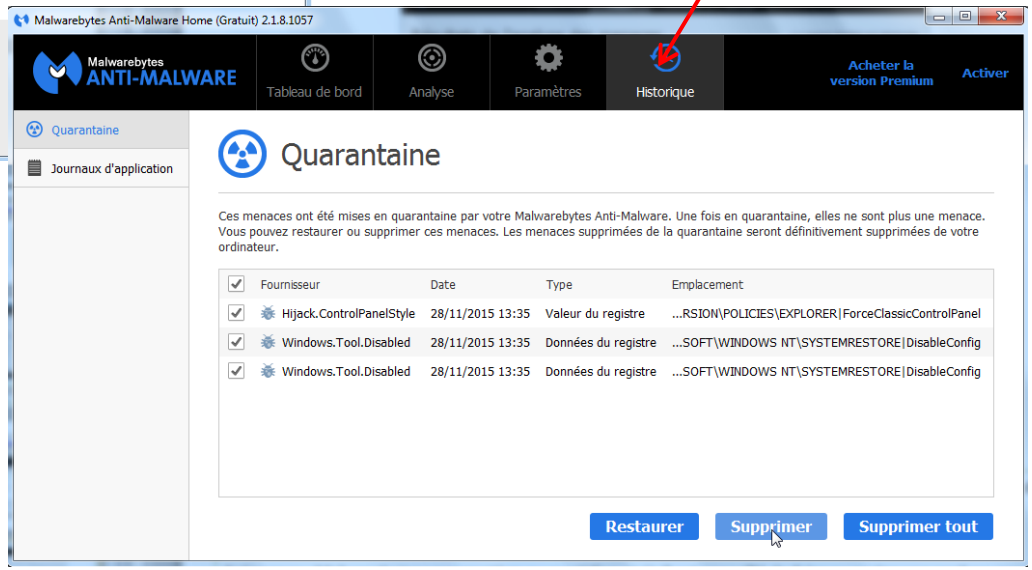
Malwarebytes s'installe comme n'importe quel logiciel. Vous double-cliquez sur le fichier téléchargé et cliquez sur « suivant » jusqu'à ce qu'il soit totalement installé.
Pour le lancer, vous pouvez aller le chercher dans vos programmes et cliquez ensuite sur « analyser maintenant ».





L'analyse de votre ordinateur peut être plus ou moins rapide, mais en général ne dépasse pas 15min.





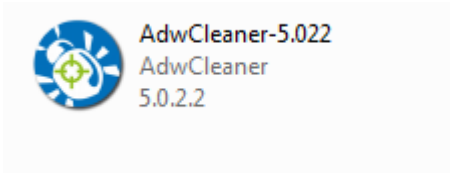
Une fois l'analyse terminée, cliquez sur « Supprimer la sélection ». Malwarebytes va vous demander ensuite de redémarrer votre ordinateur. Une fois votre ordinateur allumé, relancez Malwarebytes, et cliquez sur « Historique »pour supprimer tous les fichiers mis en quarantaine.

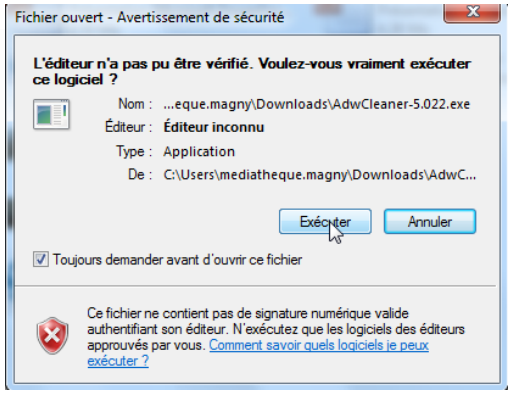
Fréquence : Malwarebytes vous protège au quotidien, mais il est conseillé de faire au moins une analyse complète par trimestre.

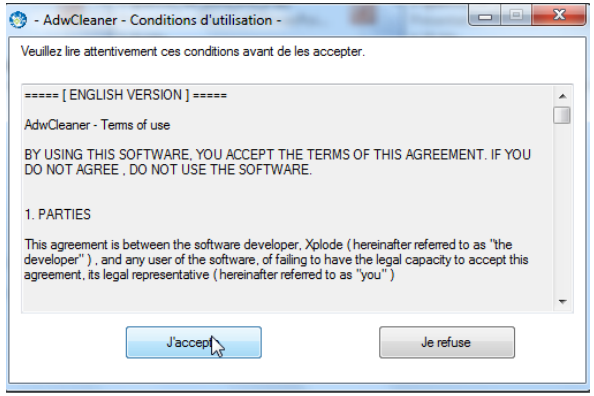
c) AdwCleaner

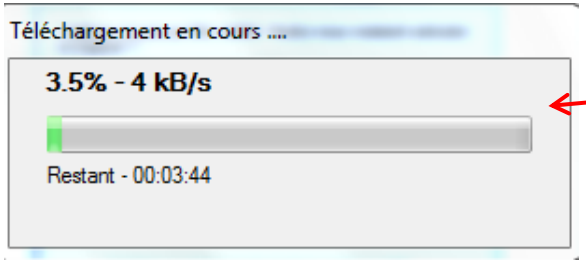
AdwCleaner est un logiciel permettant de détecter et de supprimer les malwares, c'est-à-dire les menaces pouvant potentiellement nuire au bon fonctionnement du système tels que les adwares, les toolbars (barres d'outils), les hijackers (détournement de page d'accueil) et autres programmes potentiellement indésirables. Adresse de téléchargement : http://www.commentcamarche.net/download/telecharger-34096208-adwcleaner (ou, plus simple, tapez AdwCleaner dans Google, et cliquez sur le 2e lien)

AdwCleaner a la particularité de ne pas s'installer sur votre ordinateur. Vous allez double-cliquer sur le fichier .exe , ce qui lancera le programme. Gardez-le de côté sur une clé USB pour pouvoir le réutiliser lorsque vous en aurez besoin.









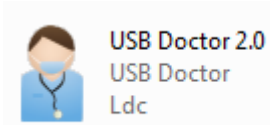
Cette étape est très rapide (quelques secondes)

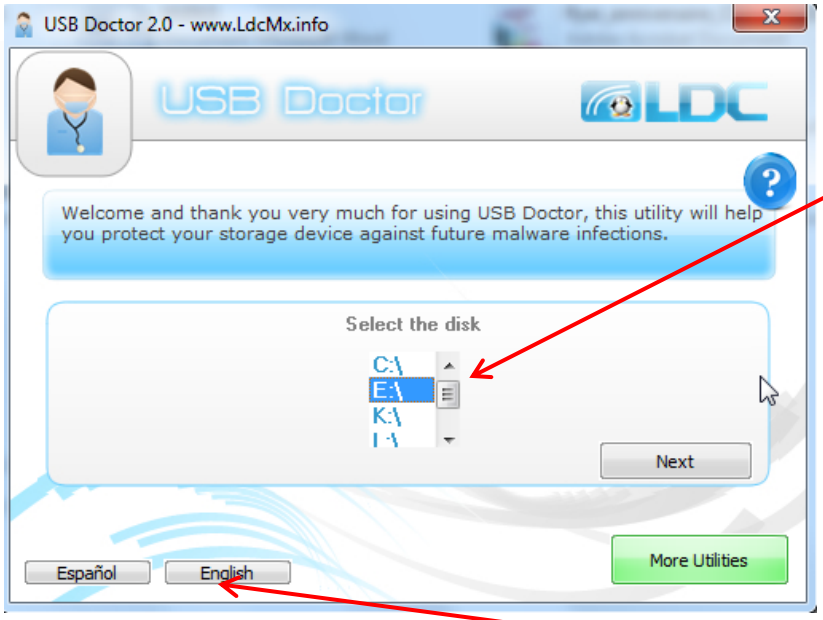
Une fois le programme ouvert, cliquez tout d'abord sur « Scanner » et ensuite « Nettoyer ». AdwCleaner va vous demander de fermer tous vos programmes et ensuite supprimer tous les parasites de votre ordinateur. Vous devrez ensuite le redémarrer. Ne vous étonnez pas de voir un rapport lorsque vous le rallumerez. Vous pouvez fermer le fichier sans risque.

Fréquence : Ponctuellement, lorsque vous constatez un problème.

d) USB Doctor

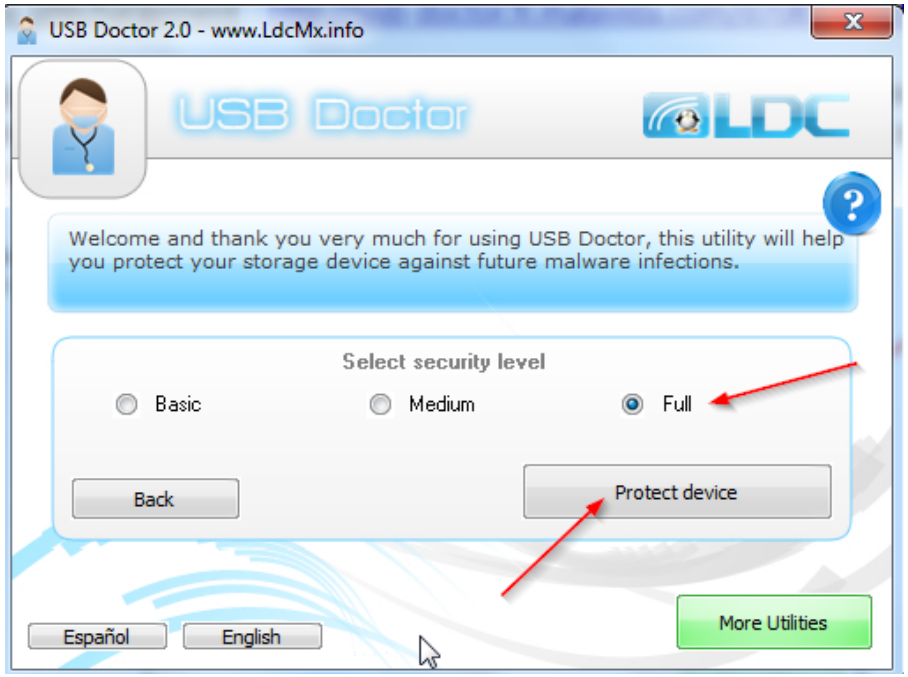
USB Doctor n’est pas un antivirus, il protège simplement les clés USB pour prévenir l'infection.
NOTE : Si votre clé USB est infectée, passez là à l’anti-virus.
Adresse de téléchargement : http://usb-doctor.fr.softonic.com/
USB Doctor a la particularité de ne pas s’installer sur votre ordinateur. Vous allez double-cliquer sur le fichier .exe , ce qui lancera le programme. Gardez-le de côté sur une clé USB pour pouvoir le réutiliser lorsque vous en aurez besoin.

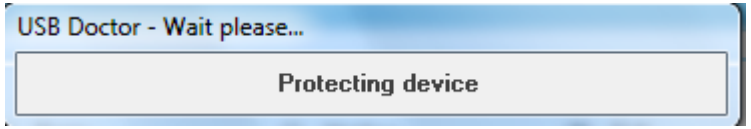


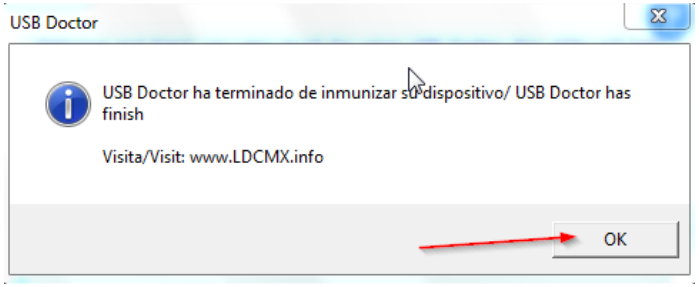


Sélectionnez le disque que vous voulez protéger et cliquez sur « Next »

USB Doctor se met par défaut en espagnol, vous pouvez changer la langue et passer en anglais







Sélectionnez « Full » pour une protection optimale et cliquez ensuite sur « Protect device ».

Fréquence : Il suffit de le faire une fois sur chacun de vos périphériques (clés USB, disques durs externes, cartes mémoires, etc.)

4. Défragmenter, restaurer, formater : connaître la différence

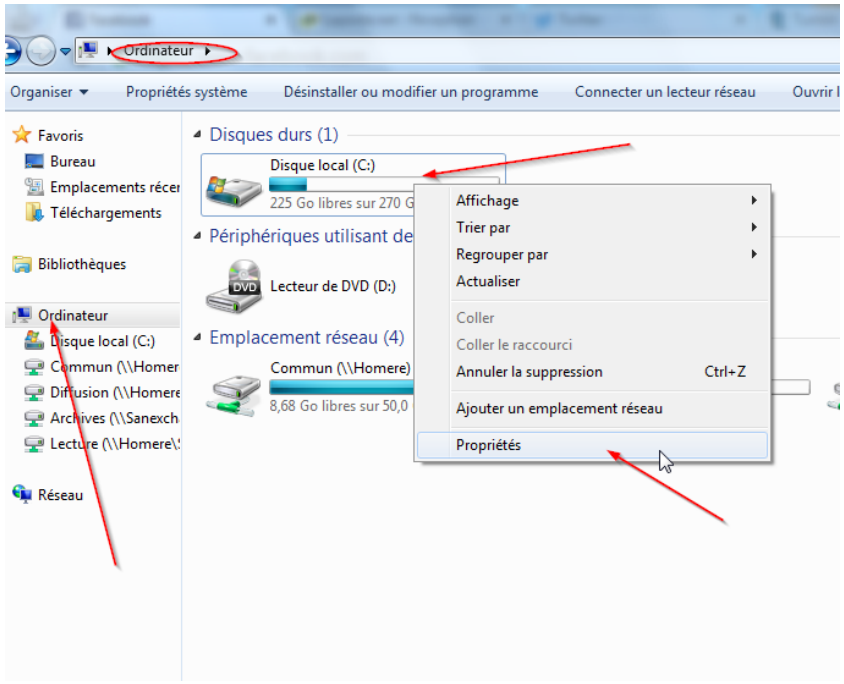
a) Défragmenter

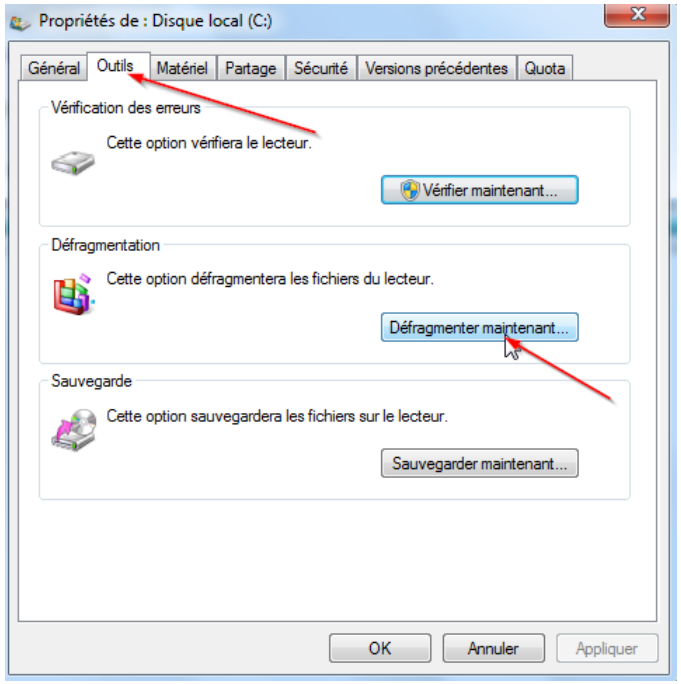
La défragmentation consiste à regrouper les fragments de fichiers éparpillés sur le disque afin d'optimiser les temps d'accès du disque dur lors de la lecture de fichiers de taille importante. Pour faire simple, défragmenter votre ordinateur permettra de le rendre plus rapide et plus efficace, mais il ne le protègera pas et n'éliminera aucun fichier infecter ou parasite.

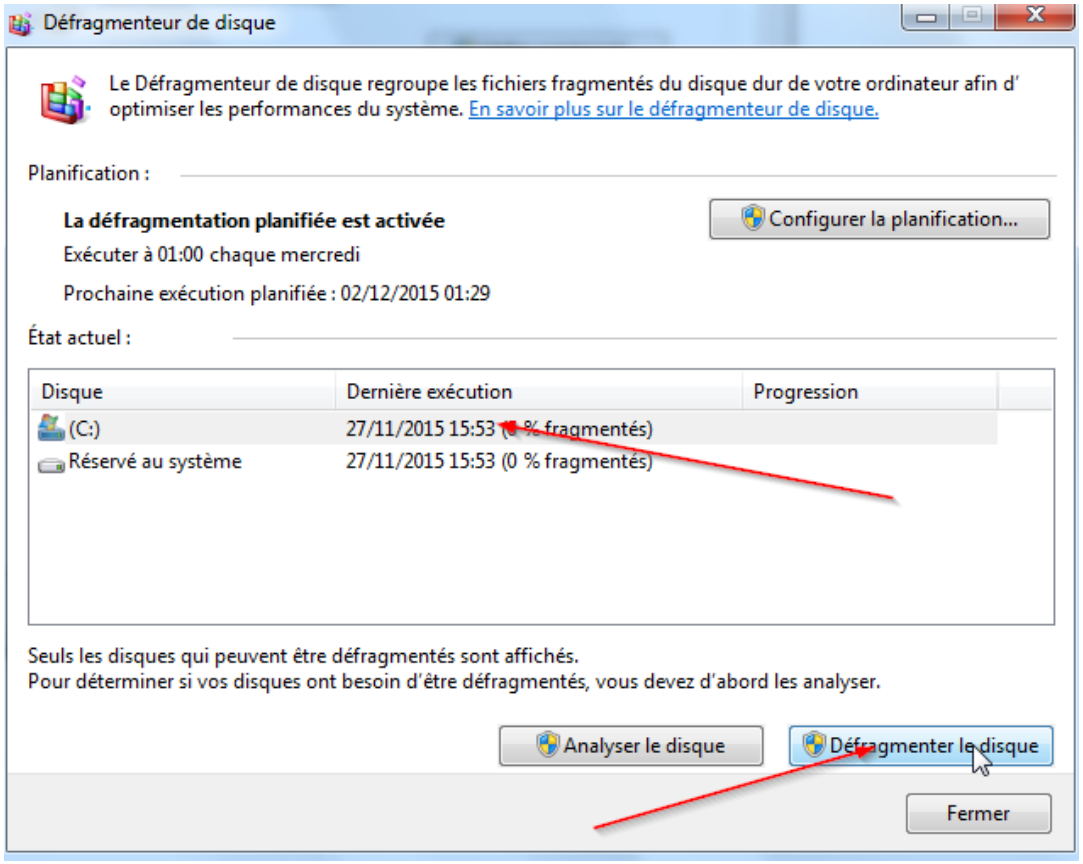
Comment faire ?

- Allez dans l'explorateur Windows, cliquez sur « Ordinateur » et faites un clic droit sur le disque C:

Cliquez ensuite sur « Propriétés ». Vous irez ensuite sur l'onglet « Outils » puis, « Défragmenter maintenant »







Une défragmentation est un long processus pouvant parfois prendre plusieurs heures, mieux vaut la lancer la nuit.

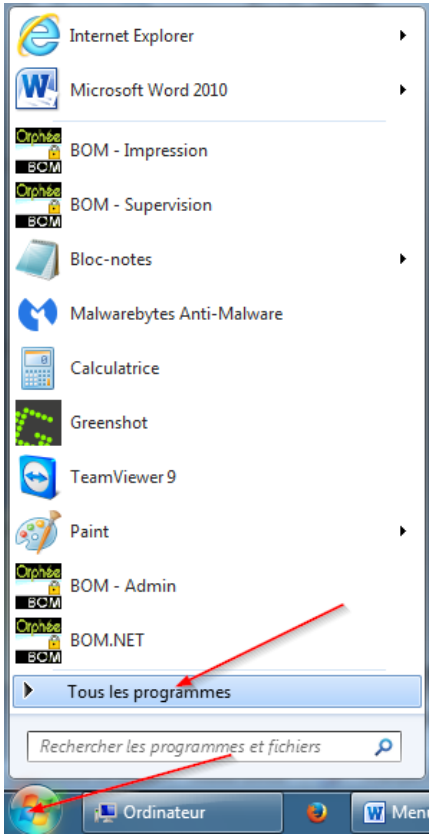
Fréquence : Une fois tous les 6 mois.

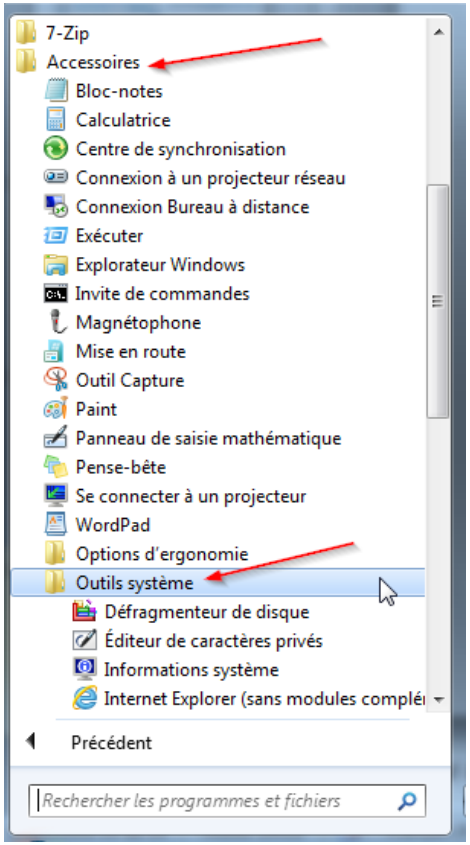
b) Restaurer

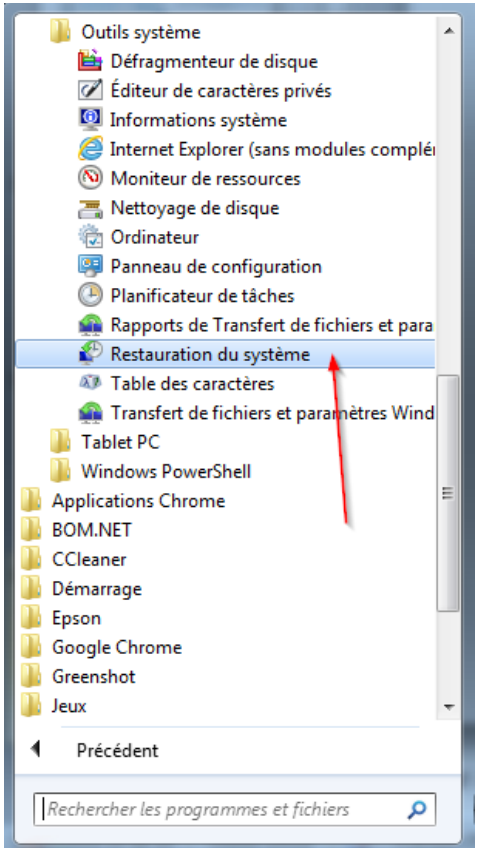
La restauration du système vous aide à restaurer les fichiers système de votre ordinateur à un point antérieur dans le temps, sans affecter vos fichiers personnels. Elle désinstallera ainsi tous les programmes (malveillants ou non) installés durant un laps de temps défini.

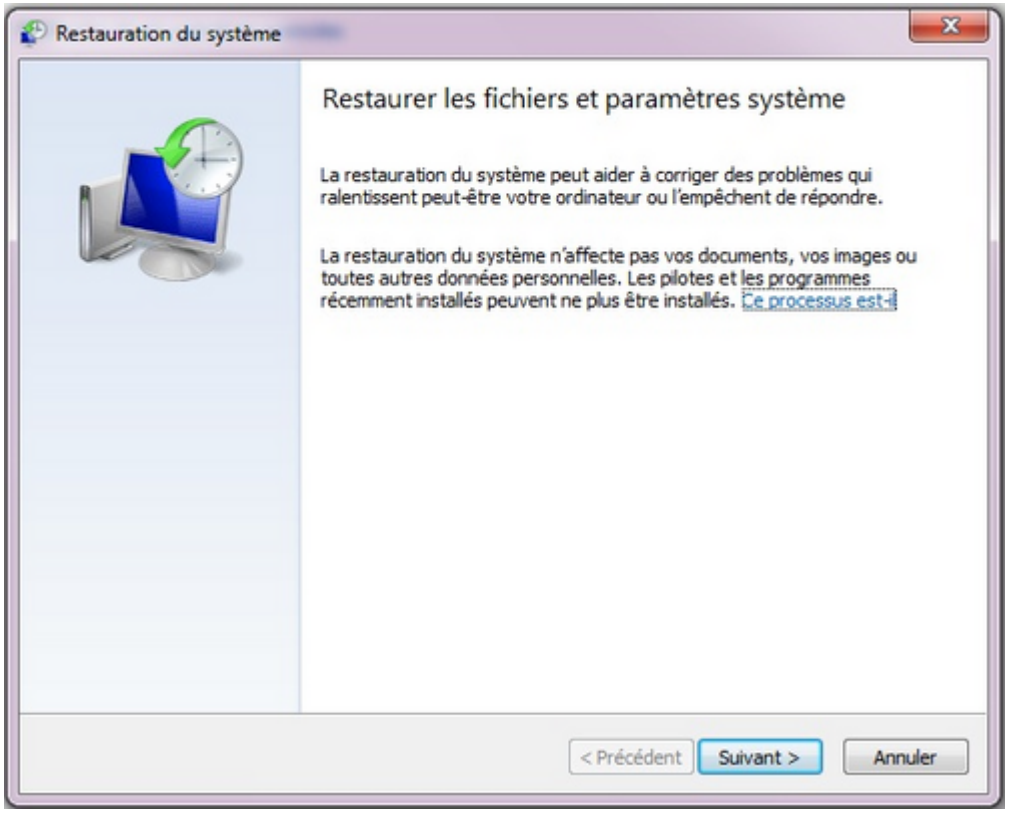
Comment faire ?

- Sur Windows 7 : Cliquez sur : Démarrer → Tous les programmes → Accessoires → Outils système → Restauration système.









- Si la date indiquée vous convient, cliquez sur **Suivant**.
- Sinon, cochez **Choisir un autre point de restauration** puis cliquez sur **Suivant**.
- Choisissez une date sur la liste, puis cliquez sur **Suivant**.
- Cliquez sur **Terminer**.

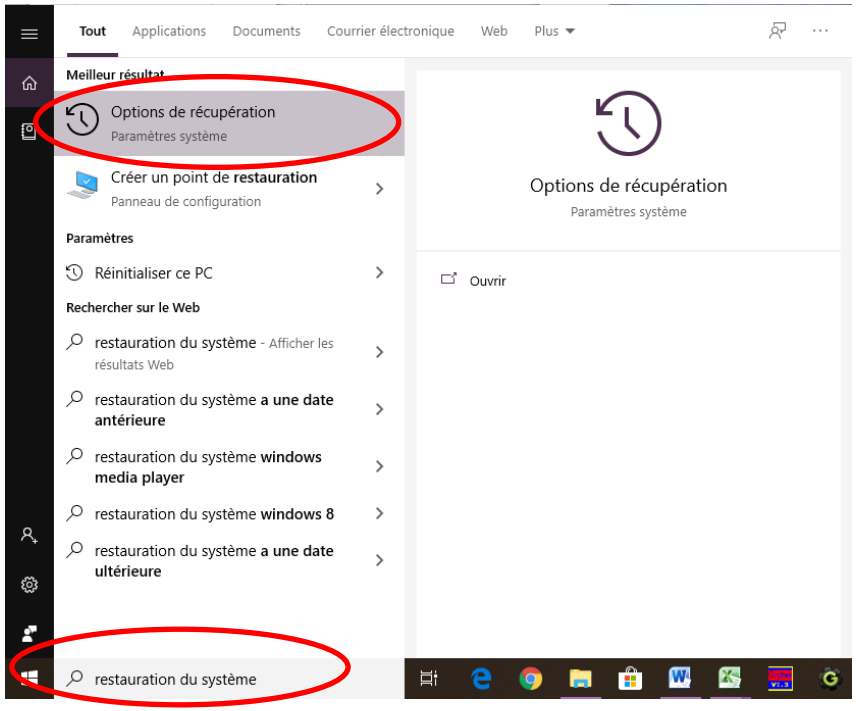
La restauration système devrait commencer.

À la fin, votre PC va redémarrer pour continuer la restauration.

Fréquence : Uniquement en cas de problème que vous ne parvenez pas à résoudre.

Comment faire ?

- Sur Windows 10 : Chercher **restauration système** et cliquer sur **Option de récupération.** Vous pourrez alors comme sur Windows 7 lancer une restauration à un point de sauvegarde ou créer un nouveau point.



c) Reformater

Après avoir installé et désinstallé un grand nombre d'applications, le système Windows devient de plus en plus lourd et instable. Lorsque les utilitaires de nettoyage ne permettent plus de revenir à un état normal ou que votre ordinateur est trop infecté pour que les antivirus en viennent à bout, il reste la solution du formatage. Le formatage d'un disque dur va supprimer toutes vos données. Attention donc à bien **sauvegarder** sur un autre support vos documents importants (textes, photos, carnets d'adresses, favoris internet…). **Ce qui ne l'a pas été sera irrémédiablement perdu après le formatage.**

Il faut également que vous possédiez un disque de formatage Windows (ou une clé USB), vous ne pourrez pas reformater sans. (fourni avec votre ordinateur à l'achat normalement)

Comment faire ?

- Démarrez votre ordinateur et insérer immédiatement le CD
- Appuyez sur une touche du clavier pour indiquer que vous voulez démarrer à partir du CD
- Suivez les indications à l'écran

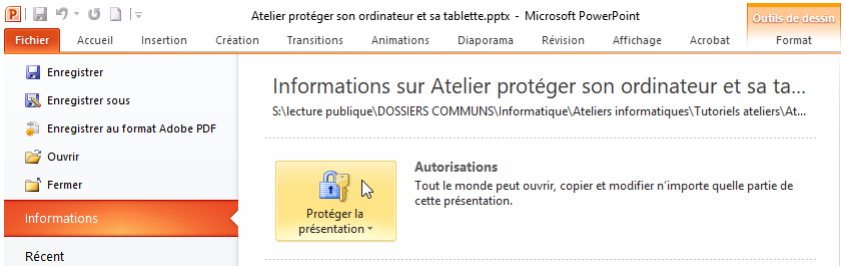
NOTE : Depuis Windows 7, il est assez difficile de reformater car beaucoup d'ordinateur ne sont plus vendus avec le disque de formatage. Il est toujours possible de le faire mais il vous faudra l'acheter à part.
Il est donc conseillé de privilégier la restauration et de ne se lancer dans un formatage qu'en dernier recours.

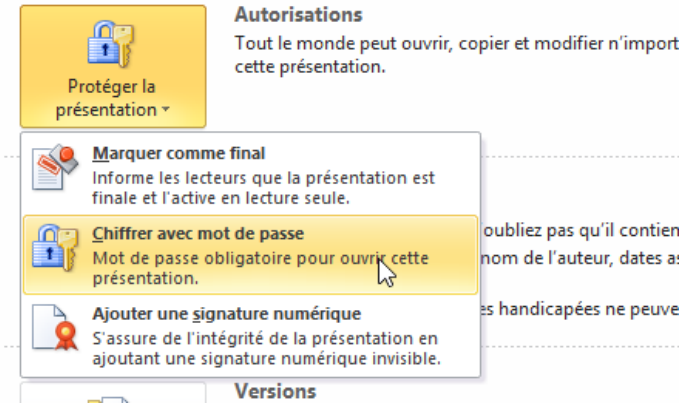
6. Protéger un document avec un mot de passe

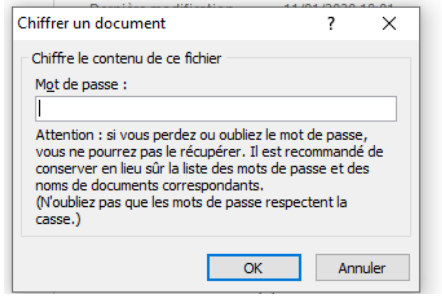
a) Protéger un document word, excel ou powerpoint

La suite Microsoft Office est équipée d'un système permettant de protéger n'importe quel document en le chiffrant avec un mot de passe.

L'option est disponible dans l'onglet **Fichier.** En cliquant sur **Protéger la présentation/le document/le classeur** vous pouvez alors définir un mot de passe.



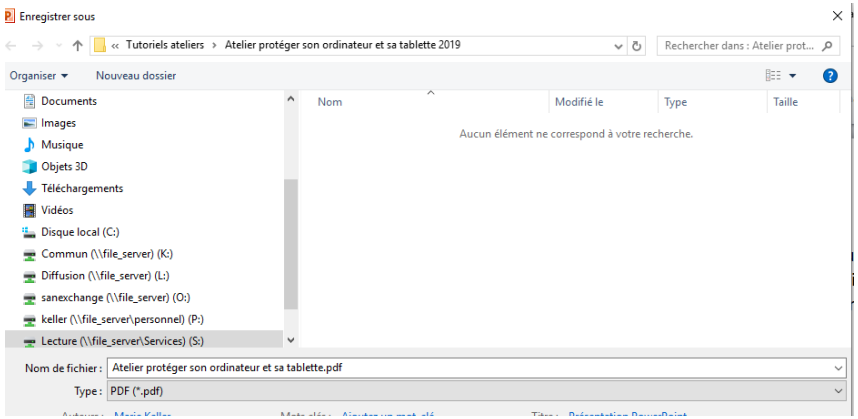


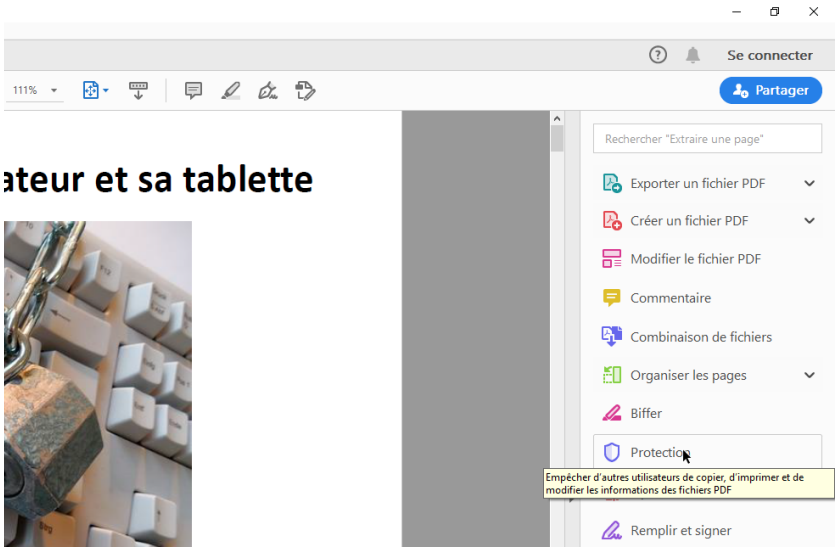


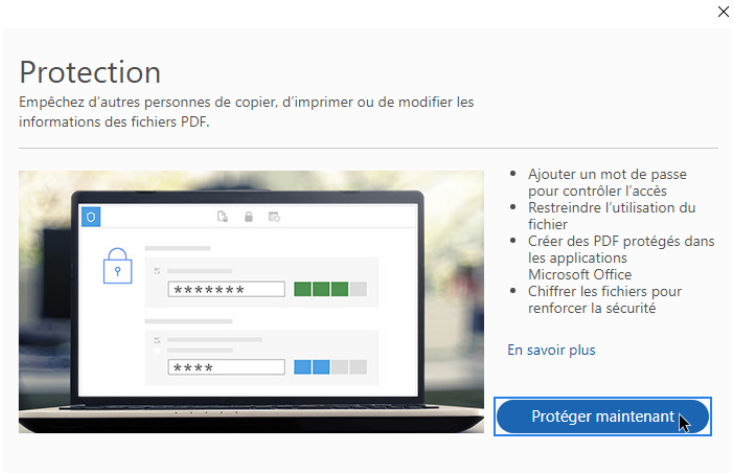
Vous pouvez aussi le **Marquer comme final**, ce qui ne permettra de l'ouvrir qu'en Lecture seule et interdira toute modification.

a) Protéger un document pdf

Lorsque vous créez un document PDF, vous avez la possibilité de protéger.
Après avoir fait **Enregistrer sous** et sélectionné le mode PDF, vous pourrez alors ouvrir le document avec votre gestionnaire de PDF (ici Acrobat reader DC) et vous pourrez alors accéder à ses propriétés de protection.



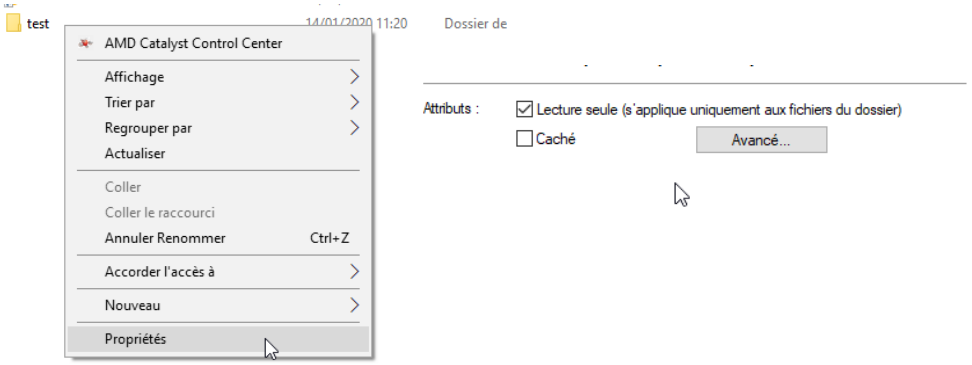


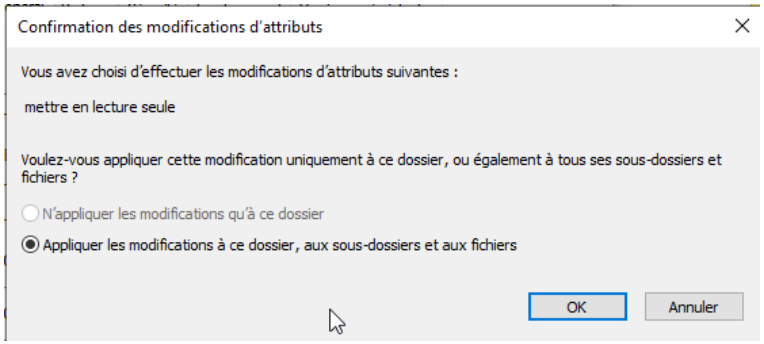


Note : les options de base sont gratuites mais nécessitent tout de même de se créer un compte avec Acrobat reader DC.

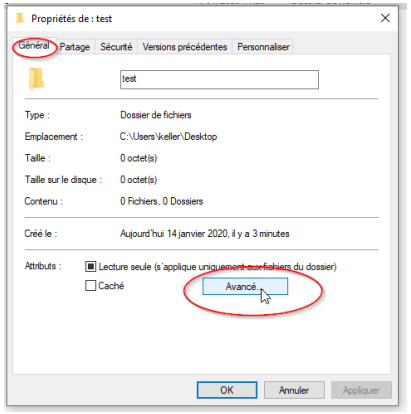
7. Protéger un dossier

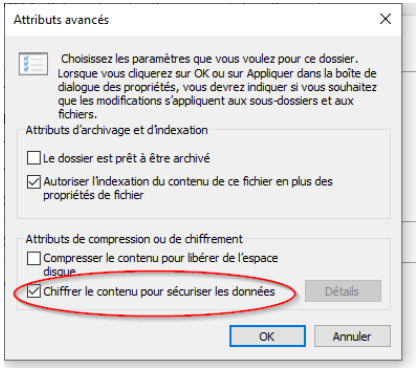
Windows 10 offre désormais nativement la possibilité de sécuriser un dossier ou un fichier. Pour ce faire, il suffit de créer le dossier, puis de faire un clic droit dessus et de choisir **Propriétés**. Vous pouvez alors décider de mettre l'ensemble des documents du dossier en **Lecture seule.**





Pour une protection plus avancée, par exemple dans des dossiers partagés sur un serveur, allez dans l'onglet **Général**, choisir ensuite **Avancé** et cochez **Chiffrez le contenu pour protéger les données**. Vous serez alors le seul à pouvoir consulter le dossier.





Note : protéger un dossier sous Windows avec mot de passe s'avère compliqué. Il faut créer un fichier .txt dans le dossier à protéger et y rentrer un script bien précis, avant d'en changer l'extension .bat. Vous pouvez retrouver la procédure exacte ici : https://www.commentcamarche.net/faq/426-proteger-un-dossier-par-mot-de-passe

Partie 2 : Protéger son portable et sa tablette

1. Antivirus, antimalware, nettoyage

Votre téléphone portable et votre tablette sont tout aussi susceptibles d'être piratés que votre ordinateur portable. Pourtant, peu nombreux sont les gens qui leur installe un antivirus et un antimalware, alors que ces derniers existent presque tous sous la forme d'applications (gratuites ou payante suivant la formule).

Quelques applications fiables que vous pouvez installer aussi bien sur Androïd qu'IOS :

- **Avast** : antivirus libre et gratuit 
- **Malwarebytes** : antimalware 
- **Ccleaner** : outil de nettoyage 

Il est conseillé de lancer ces applications au minimum une fois tous les 2 ou 3 mois.

2. Sécuriser par mot de passe/schéma/emprunte digitale

Le verrouillage est la **première barrière de sécurité** contre une utilisation frauduleuse de notre smartphone. Il peut s'agir d'un **code de verrouillage**, d'un **modèle à tracer**, d'une **lecture d'empreintes digitales** ou même d'une **lecture de l'iris**. Ces méthodes ont leurs avantages et leurs inconvénients.

On conseille habituellement, le code de verrouillage ou l'emprunte qui sont les plus fiables.

Pour modifier ces réglages, il vous faudra vous rendre dans les **Paramètres** de votre appareil, puis dans la rubrique **Ecran verrouillage/Sécurité.**

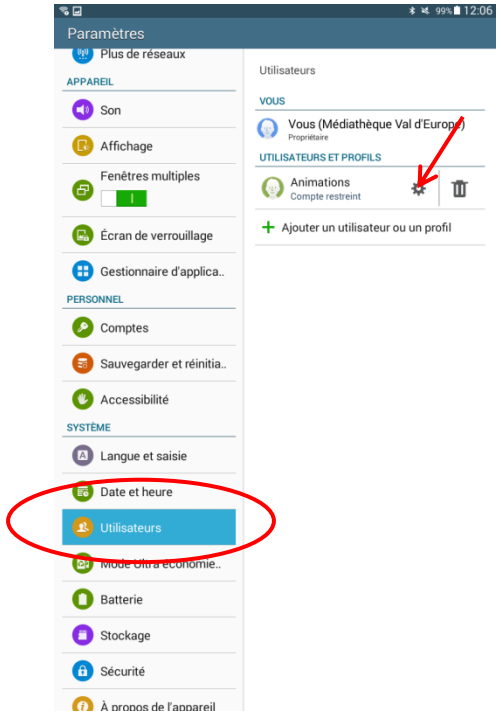
3. Créer des profils spécifiques

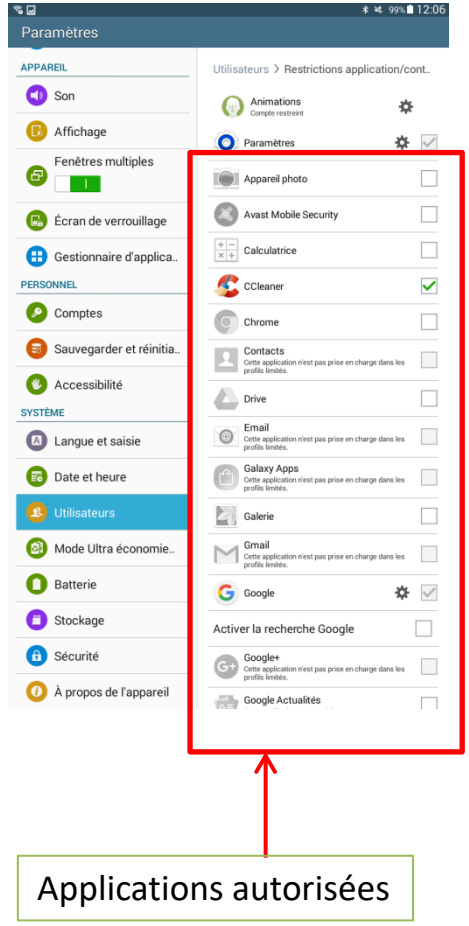
La plupart des appareils mobiles permettent de créer des profils spécifiques pour éventuellement bloquer l'accès à certaines applications et aux paramètres de l'appareil si vous le prêtez.

→ Ouvrez l'application **Paramètres** de votre appareil.
→ Appuyez sur **Utilisateurs** et **Comptes Utilisateurs**.
→ Appuyez sur **Ajouter un utilisateurs** puis **OK**.

- Si l'option **Ajouter un utilisateur** ne s'affiche pas, appuyez sur **Ajouter un utilisateur ou un Profil Utilisateur** puis **OK**.
- Si aucune de ces options ne s'affiche, cela signifie qu'il n'est pas possible d'ajouter des utilisateurs sur votre appareil.

Vous pouvez ensuite configurer le nouveau compte utilisateur en allant dans ses **paramètres**.





4. Bloquer les sources non sûres

Le vecteur d'infection numéro 1 des appareils mobiles est l'installation d'applications venant **de sources non sûres**.

Les applications Android terminent typiquement par l'extension ".apk" et rien n'empêche de partager une telle application via un site web donné hors du *Play Store*.

Le blocage est habituellement mis en place par défaut sur la plupart des appareils. Vous pouvez tout de même vérifier sur le vôtre. Allez dans les **Paramètres** et dans les **Options de sécurité**.

5. Chiffrer ses données & les sauvegarder

Il s'agit aussi de fonctionnalités plus ou moins par défaut, mais si votre téléphone n'est pas doté de cette option, vous pouvez utiliser des applications spécialement conçues pour cela.

→ SSE Universal Encryption App
→ Cybersafe Chiffrement

Ces applications permettent de :

- Stocker et gérer ses mots de passe
- Chiffrer des messages au format texte
- Chiffrer des fichiers ou dossiers
- Créer des coffres fort numériques
- Etc.

Il est également important de penser à sauvegarder régulièrement vos données afin de pouvoir les récupérer en cas de vol, perte ou piratage.

Vous pouvez le faire manuellement pour vos images, vidéos, etc., mais pour le reste (mail, sms, etc.) vous devez passer par une application comme **Super Backup SMS & Contacts**.

6. L’importance de mettre à jour

Il s’agit de l’un des points les plus **importants**. Mettre à jour son téléphone et les applications permet de corriger les vulnérabilités. On imagine trop souvent que mise à jour rime avec “nouvelle fonctionnalité” alors qu’il s’agit également (et surtout !) de **patcher le mobile ou l’application contre des failles**.

La mise à jour **nous concerne également**, se tenir informé(e) des menaces est un excellent moyen pour ne pas tomber dans un piège à l’avenir. 90% des piratages réussis exploitent en fait la faiblesse de l’être humain.

Pensez donc à mettre à jour votre téléphone.

Le mot de la fin : L'art du mot de passe

- Evitez l'évidence (date de naissance, code postal, adresse, noms des enfants,…)
- Combinez lettres (majuscules et minuscules), chiffres et caractères spéciaux. Ex: V1veL@MV3
- Ayez au moins un mot de passe de 8 caractères (il faudrait 66 ans à une machine spécialisée pour craquer un bon mot de passe de 8 caractères)
- Prenez une phrase comme moyen mnémotechnique. Ex: l1f0rm@tikCc00L (l'informatique c'est cool)
- Changez au moins une fois par an vos mots de passe (une fuite est si vite arrivée)
- N'utilisez pas le même mot de passe partout. Vous pouvez réutiliser la même base, mais personnalisez le en fonction du site ou document que vous voulez protéger. Ex: FB l1f0rm@tikCc00L pour Facebook et TTl1f0rm@tikCc00L pour Twitter
- Ne vous faites pas de mémo !! (clavier, portefeuille, etc.). Ou alors, créez vous un fichier que vous protègerez par… un mot de passe. (mais ce n'est pas vraiment conseillé non plus)
- Sur Internet, ne cochez pas la case « rester connecter » ou « identification automatique »