Quand nos ordinateurs tombent malades

M X se croit bien protégé, il a un très bon antivirus qui lui coûte 60€/an. Pourtant un matin, son PC affiche une page de ce genre :

Et il ne peut plus rien faire d'autre !!!

Pour d'autres ce sera moins bloquant mais plus insidieux, la machine est très lente, l'accès à Internet est impossible, certains programmes ne fonctionnent plus etc....

Comment cela est-il possible avec un super antivirus ?

Il faut comprendre qu'un antivirus, aussi performant soit-il ne peut bloquer que les virus connus, grâce à une liste de signatures de virus qu'il met à jour quotidiennement, voir plusieurs fois par jour.

Cependant lorsqu'un nouveau virus est lâché dans la nature, il s'écoule un certain temps avant que les éditeurs de logiciels antivirus ne l'aient identifié et n'aient distribué sa signature. Si par malchance vous êtes contaminés pendant ce temps de latence, votre antivirus ne vous sera d'aucune aide puisque à cet instant, il ne connaît pas ce virus et ne peut donc le bloquer.

Cependant dans 3 ou 4 jours, voire une semaine, la situation sera différente, car tout le monde connaîtra la signature de ce virus et elle sera distribuée à votre machine, mais pas de chance, le virus est installé sur votre PC.

Rien n'est encore perdu, car votre antivirus possède une botte secrète : **Le scan local.**

Le **Scan local**, c'est un programme, livré avec tout antivirus, qui parcourt tous les fichiers de votre mémoire et de votre disque dur et vérifie qu'ils ne sont pas infectés par un des virus dont il connaît la signature, auquel cas il vous alerte et vous propose :

- soit de réparer le fichier (quand c'est possible)
- soit de le mettre en quarantaine
- soit de le supprimer
- soit autre chose (suivant votre antivirus)

Malheureusement, à moins que vous ne l'ayez paramétré, le **Scan local** ne se déclenche pas automatiquement. C'est donc à vous de le lancer. Encore faut-il savoir le faire !!!

Il faut également savoir qu'un scan local minutieux peut durer plusieurs heures !

Donc, pas de PC sur batterie, pas de scan local si risque de coupure de courant (Orage), pas de scan local si vous avez besoin de la machine dans 10 minutes ou si vous partez dans une demi-heure,,,,

ATTENTION : Un seul antivirus doit être installé sur une machine. Deux antivirus ne peuvent fonctionner en même temps sur un PC sous peine de gros dysfonctionnements et d'un ralentissement important de la machine qui peut aller jusqu'à la rendre inutilisable

N'y a-t-il pas un moyen de se protéger plus efficacement

Si un virus a pu agir c'est qu'il en avait le droit. Et pourquoi en avait-il le droit ?: parce que **votre compte utilisateur est un compte Administrateur !!!!**
En effet quand vous installez Windows, le premier compte que vous créez et un compte Administrateur, pour que vous ayez la possibilité de gérer votre machine.
Le problème, c'est que ce compte est un laissez-passer pour les virus, puisqu'il a tous les droits. Donc il ne devrait jamais être utilisé et Windows devrait vous obliger à créer dans la foulée un compte Utilisateur qui ne soit pas administrateur et qui ait des droits limités sur la machine. Malheureusement, Windows ne vous oblige pas à faire de la sorte, et c'est pour cela que 99 % des utilisateurs de Windows (hors entreprises) travaillent avec un compte Administrateur, ce qui est la porte ouverte aux virus, Malwares et autres problèmes.
Le plus beau de l'histoire, c'est que lorsque vous créez un nouveau compte sous Windows, on vous vante les mérites du compte Utilisateur et on vous explique pourquoi un compte utilisateur devrait être utilisé au lien d'un compte Administrateur !!

Sous Linux, ce problème n'existe pas, car même si vous êtes administrateur de votre machine, dès qu'une action risque de toucher à votre système d'exploitation, il vous est demandé le mot de passe administrateur. Même en mode commande certaines actions ne peuvent être accomplies qu'avec un profil administrateur qui nécessite le mot de passe (C'est le fameux Sudo ..).

Vous aurez donc compris la supériorité d'un tel système. Sans le mot de passe tout logiciel malveillant sera bloqué avant d'avoir pu faire quoi que ce soit de dommageable

Quelles sont les restrictions du compte utilisateur sous Windows ?

Eh bien peu et beaucoup !!

Beaucoup, parce que dès que vous voudrez entreprendre une action qui risque de modifier le système, il vous sera demandé le mot de passe administrateur, voir indiqué que cette action n'est réalisable que sous le profil administrateur (exécuter en tant qu'Administrateur)

Peu, parce que taper le mot de passe Administrateur, même cinq fois par jour, c'est pas la mort et c'est le prix à payer pour la sécurité.

Quand vous quittez votre maison, je suppose que vous fermez la porte à clé !C'est une contrainte parce qu'il faut sortir les clés , fermer la porte, ranger les clés et si vous rentrez le soir sous la pluie, il faut à nouveau sortir les clés ouvrir la porte....Ce serait plus simple si la porte était restée ouverte !!!
Et plus simple pour les cambrioleurs aussi !!!

Ok j'ai compris la leçon, Comment mettre mon ou mes profils en utilisateur ?

C'est relativement simple et rapide et cela se passe en trois étapes :

- Créer un compte administrateur que vous nommerez comme vous voulez, sauf « Administrateur » et qui aura bien sur un profil administrateur
- Lui attribuer **un mot de passe difficile à craquer** (donc 8 caractères minimum et pas le nom du chien ou des enfants)
- Se déconnecter de son compte et se signer sous ce compte « Administrateur » qui vient d'être créé
- Modifier tous les autres comptes pour les mettre avec un profil « utilisateur »
- En profiter pour créer un compte « Famille » qui sera utilisé par vos enfants ou petits enfants et éviter ainsi qu'après leur visite votre machine soit inutilisable !!
- Se déconnecter du compte Administrateur
- Se connecter avec votre compte habituel qui est maintenant un compte utilisateur
- Ne plus jamais utiliser le compte Administrateur sauf cas de force majeure
- A partir de là, chaque fois que l'ordinateur aura besoin des droits « Administrateur » pour exécuter un programme ou une action spécifique, une fenêtre s'ouvrira en vous demandant le mot de passe « Administrateur ». Avant de le renseigner vérifier que le programme qui demande ces droits à bien été lancé par vous. Dans le cas contraire ne mettez pas le mot de passe et faites annuler pour fermer la fenêtre

Y a-t-il d'autres astuces pour protéger mon ordinateur ?

Quelques règles simples qui vont vous faire comprendre que **le meilleur anti-virus, c'est vous** :

- Mettre **ADBLOCK+**[1] sur votre navigateur, vous évitera les fenêtres de pub et la tentation de cliquer là ou il ne faudrait pas
- Prendre le temps de lire ce qui est écrit à l'écran avant de cliquer
- Ne pas cliquer sur tout ce qui bouge
- **Garder votre système à jour** grâce aux mises à jour de Windows Update et à celle des logiciels critiques tels que FLASH player, Adobe reader, Java, etc,,,
- S'abonner à la lettre de sécurité de SECUSER : http://www.secuser.com/newsletters/index.htm#secuser_securite
- Utiliser un logiciel pour gérer votre courrier (THUNDERBIRD est un des meilleurs) vous évitera de rester en ligne pendant des heures et donc vulnérable
- Activer si ce n'est déjà fait un pare-feu (celui de Windows par exemple)
- Ne mettez pas de mots de passe simples et surtout pas le même pour tout
- Faire des sauvegardes de vos données personnelles **tous les jours** avec un logiciel de synchronisation (FREEFILE SYNC) et une image disque tous les 6 mois
- Utilisateurs de Windows, créer de temps en temps des points de restauration peut vous tirer d'un mauvais pas !!

J'arrête ici la liste et je précise à tous ceux qui sont encore sous **Windows XP** que Microsoft a arrêté la mise à jour de ce système en avril 2014, et que si vous ne l'avez pas encore compris, **un système non mis à jour est très vulnérable !!**

La gestion des comptes utilisateurs sous Windows

Bien que votre Ordinateur soit appelé « Ordinateur Personnel » ou PC (Personal Computer), c'est pas vraiment comme une brosse à dent, **ça se prête**. Du coup la tendance et de parler maintenant d'ordinateur Familial.

Le problème se pose alors de la personnalisation et surtout de la sécurité car vous n'avez pas forcément envie qu'après le passage de vos enfants ou petits enfants sur votre PC , celui-ci devienne inutilisable car votre bureau a changé ou pire que suite à des navigations hasardeuses sur internet, votre machine soit devenue instable, ou lente, ou pire encore

Heureusement les systèmes d'exploitation modernes proposent la création de comptes utilisateurs, qui permettent de personnaliser sa session de travail, sans interférer avec celles des autres utilisateurs. Hérité de la gestion des réseaux d'entreprise cette création de comptes permet aussi de gérer les droits des utilisateurs, tant sur les fichiers que sur le matériels ? C'est d'ailleurs principalement la puissance de gestion de ces droits qui différencie les versions familiales et professionnelles de Windows.

Quand les droits sont limités, on parle de **compte UTILISATEUR** et quand il n'y a aucune restrictions, on parle de **compte ADMINISTRATEUR**.

Là ou les choses se dégradent, c'est que Microsoft n'a pas jugé utile d'obliger les utilisateurs à ne pas travailler avec un compte administrateur, ce qui est une grosse lacune au niveau sécurité, et vous allez comprendre pourquoi.

1 Depuis que l'on sait que ADBLOCK fait payer pour sa liste blanche, lui préférer UBLOCK qui a le bénéfice du doute !!!

Imaginez que vous partez en vacances et laissez la maison à un couple de retraités. Vous ne les connaissez pas plus que ça et donc vous avez le choix de leur laisser un passe partout qui ouvre donc toutes les pièces de la maison ou bien les clés des seules pièces qui leur seront utiles pendant leur séjour : leur chambre, la cuisine et les Wc/Salle de bain. Les autres pièces de la maison seront verrouillées et ils n'en auront pas les clés
Si pendant votre absence ces braves gens sont victime d'un agresseur, celui ci ne pourra ouvrir que les pièces dont il aura volé les clés. Si vous avez laissé un passe partout, il aura accès à toute la maison !!

Eh bien pour votre ordinateur c'est un peu la même chose, si vous travaillez avec un compte ADMINISTRATEUR, vous avez des droits sur tous les Fichiers et dossiers de votre ordinateur et donc si un virus (c'est l'agresseur) s'active sur votre machine, il hérite de ces droits et peut donc faire des dégâts non seulement sur vos fichiers mais aussi sur les fichiers système de votre machine

Cependant, si vous travaillez avec un **compte UTILISATEUR**, vos droits seront limités aux fichiers et dossiers que vous aurez créés et si vous voulez accéder par exemple à la base de registre, ou aux fichiers d'un autre utilisateur, ou même simplement supprimer une icône de votre bureau, le système va vous demander le mot de passe administrateur, car vous êtes seulement utilisateur, et sans mot de passe vous ne pourrez pas aller plus loin et bien sur ce sera la même chose pour un virus ou un logiciel malveillant.

Vous comprenez maintenant l'intérêt de créer plusieurs comptes et de ne jamais utiliser le compte administrateur dans une session de travail , et bien sur de protéger l'accès à ces divers comptes par un mot de passe !!!

Si j'ai bien compris, le compte administrateur ne sera jamais utilisé ?

Pratiquement jamais, car avec votre compte utilisateur vous pourrez faire des travaux théoriquement réservés à l'administrateur, sous réserve de fournir le mot de passe du compte administrateur !

Ok mais alors je vais devoir taper un mot de passe dix fois dans la journée

C'est probable, mais **c'est le prix de la sécurité**.

Quand vous quittez votre maison pour aller faire les courses, vous fermez la porte à clé. Ça veut dire sortir les clés, fermer, ranger les clés, et refaire la manip en rentrant, avec en prime les sacs de course dans une main .Pour éviter ces désagréments vous pouvez juste claquer la porte, mais il ne faudra pas vous plaindre le jour ou vous aurez été cambriolé durant votre absence avec dans ce cas impossibilité de faire jouer l'assurance !!

Alors combien faut-il créer de comptes

Au moins 2 :

- 1 compte à votre nom avec des droits *utilisateur* que vous utiliserez quotidiennement
- 1 compte Administrateur, avec des droits *administrateur*. Que vous n'utiliserez quasiment jamais

Si vous partagez la machine avec d'autres, il vous faudra en théorie créer un compte utilisateur par personne ou par groupe de personne

Vous pouvez également activer le compte Invité qui a des droits très limités et qui est tout à fait adapté lorsque vous donnez accès à votre machine à des amis qui veulent juste aller sur internet

Enfin l'avantage d'avoir plusieurs comptes (voir 2 comptes administrateur) c'est qu'en cas de problème sur un de vos comptes (ça peut arriver qu'un profil soit défectueux) vous avez encore une roue de secours en utilisant un autre compte

Pour aller plus loin :

https://openclassrooms.com/courses/debutez-en-informatique-avec-windows-7/gerer-les-comptes-utilisateurs-1

http://www.commentcamarche.net/contents/1399-windows-7-gestion-des-utilisateurs

A partir de Windows 8 se pose la question du compte local ou du compte Microsoft

Depuis Windows 10, est apparue la notion de compte Microsoft, histoire de bien verrouiller les utilisateurs à la firme de Redmond

C'est une des raisons qui à elle seule justifie de passer sous Linux, mais c'est un autre débat !

A ce jour, vous avez encore la possibilité de créer des comptes locaux, mais pour combien de temps encore ?

Ceci dit, tous les utilisateurs de smartphones sous Android ont un compte Gmail , juste pour accéder à Google Play!

Bientôt un compte chez Renault pour la bagnole, un pour les impôts, la sécu, Darty, la banque, la mutuelle....et j'en oublie.Vive Keepass[2] !!

C.CHANEL

La sécurité, c'est comme l'assurance, c'est avant l'accident qu'il faut s'en préoccuper
Sans tomber dans la psychose, dites vous bien que le piratage cela n'arrive pas qu'aux autres
Quand on voit que des géants comme Yahoo, des banques, des centres hospitaliers en sont les victimes, on n'est plus dans la science fiction. Et avec la prolifération des objets connectés et la cupidité de certains fabricants pour qui faire du fric passe avant la sécurité et la fiabilité de leurs produits, ce sera plus que jamais au consommateur de se poser les bonnes question et de gérer lui-même sa propre sécurité

2 Logiciel de gestion des mots de passe