BSCI
Bertrand SCHMERBER
Conseil en Informatique

La sécurité numérique
Stratégie de sécurité du PC

Les pirates sont rarement très persévérants, ils préfèrent les proies faciles aux défis technologiques, et internet regorge d'ordinateurs personnels ouverts aux quatre vents dont ils peuvent prendre le contrôle à distance en quelques minutes.

Heureusement il n'est pas nécessaire d'être un expert pour bien protéger son PC. Quelques astuces simples, des logiciels gratuits et un peu de bon sens suffisent à protéger convenablement votre PC.

Voici mes conseils pour assurer une bonne sécurité pour votre PC, des données qu'il contient et de vos données personnelles

1. Le comportement à suivre pour ne pas chercher les ennuis

Le virus le plus dangereux est parfois assis juste en face de l'écran !

Il faut toujours respecter les règles de bases de la sécurité

- **Éteindre l'ordinateur lorsqu'il n'est pas utilisé**
- **Ne partager ni disques ni imprimantes sur Interne**
- **Ne pas utiliser de programme ou de fichier de provenance douteuse**
- **Ne jamais ouvrir un Mail d'origine inconnue, Ne répondez et ne cliquez pas sur un lien si vous n'êtes pas 100% certain de connaitre l'expéditeur**
- Ne rangez pas vos copies de sécurité près de l'ordinateur
- Surveiller les performances de sa machine

Protégez aussi votre confidentialité en ligne

- Évitez de publier des informations personnelles sur les réseaux sociaux. Par exemple, votre date de naissance est souvent utilisée comme identifiant ou question de sécurité. Évitez donc de la rendre publique.
- Vos comptes de réseaux sociaux doivent rester privés. Seuls vos amis et les membres de votre famille peuvent y accéder.
- Évitez de répondre à des questionnaires ou de participer à des cagnottes en ligne, qui capturent souvent des données personnelles.
- Conservez uniquement les comptes en ligne que vous utilisez réellement.
- Pour limiter le suivi, utilisez un navigateur Web qui inclut un logiciel de blocage de trackers et des publicités.
- Vous pouvez utiliser un VPN (Virtual Private Network) pour renforcer votre confidentialité en ligne. Grace au VPN, votre adresse IP reste cachée et les données échangées seront chiffrées. Cela empêche complique considérablement la vie des cybercriminels

Sachez que la paranoïa n'est pas une bonne méthode de sécurité, et comme il vaut mieux de prévenir que guérir, Il faut mettre en place de la sécurité

2. Les principes du plan de sécurité

Après avoir évalué les risques il est possible de prendre des mesures pour réduire le danger, et les 4 premiers points sont absolument indispensables

- **Installez un antivirus (Avira Antivir dans la version gratuite est excellant)**
- **Utilisez un firewall (pare-feu)**
- **Utilisez périodiquement un anti-spyware**
- **Faites des sauvegardes automatiques**
- N'utilisez pas un compte administrateur pour le travail quotidien
- Partitionnez votre disque dur, ça facilite la maintenance
- Clonez de la partition contenant Windows et les programmes
- Faites les mises à jour de sécurité de Windows
- Contrôlez de temps en temps votre sécurité

Vous pouvez maintenant installer tous les programmes dont vous aurez besoin. Mais un conseil, si vous installez des programmes « gratuits » faites un nouveau passage de votre anti-spyware, vous pourriez avoir des surprises.

• Installez un antivirus

Installer un antivirus est indispensable à partir du moment où vous échangez des documents entre votre PC et un autre PC quel que soit le support. C'est même vital si vous avez une connexion internet.

Des codes dangereux (chevaux de Troie, virus etc.…) peuvent se cacher dans les pages d'un site web ou dans un document que vous ouvrez (image, musique, courrier etc..), et surtout dans un petit programme amusant que vous recevez d'un ami ou que vous téléchargez gratuitement

Une fois l'antivirus installé, pensez à activer la mise à jour automatique et vérifiez de temps en temps que le programme fonctionne correctement (Je vous recommande vivement **Avira Antivir** dont la version gratuite est déjà très efficace)

• Utilisez un pare-feu

Lorsque vous êtes en réseau, vous isolez votre PC du monde extérieur en utilisant un pare-feu. Ce type de programme agit comme un garde-barrière et contrôle les tentatives de connexions à votre ordinateur. Il contrôle quelles applications installées sur votre disque dur ont le droit de se connecter à l'internet.

Windows possède un pare-feu intégré, et depuis Windows 7 il est devenu suffisamment efficace pour un usager standard. **Il est toujours activé par défaut** et le **moniteur de sécurité de Windows** vous signale une éventuelle désactivation accidentelle ou malveillante.

De plus votre « Box » qui vous donne accès à internet intègre un second pare-feu lui aussi active par défaut. Là aussi les versions les plus récentes sont suffisamment efficaces, mais pour éviter qu'un pirate ne le désactive il faudrait au moins

commencer par donner à votre box un mot de passe personnalisé (voire dans le mode d'emploi de la box)suffisamment complexe (au moins 10 à 12 caractères)

- **Utilisez périodiquement un antispyware**

"Spywares" et "Adwares" sont devenus les deux nuisances parmi les plus répandues. Ce sont des logiciels clandestins installés en même temps que des applications (souvent gratuites) que vous téléchargez sur l'internet. Ce sont des logiciels espions dont le rôle est de collecter des données confidentielles sur votre ordinateur et les transmettre aux pirates qui les ont installés, le plus souvent d'étudier vos habitudes de consommation pour renseigner les sociétés de marketing qui les installent.

De plus en plus de programmes antivirus assure aussi la protection contre les Spywares et les Adwares (comme **Avira Antivir** que je recommande),

Mais est recommandé de compléter la sécurité avec un antipsyware spécialisé, des logiciels gratuits et très efficace peuvent le faire, je recommande particulièrement **Malwarebytes** un scan mensuel avec la version gratuite sera tout à fait suffisant.

- **Faites des sauvegardes automatiques**

C'est la seule et unique solution capable de limiter au maximum les pertes de documents en cas en problème grave (Voir le chapitre conservation des informations et le programme **Fitness for Windows** que j'ai développé a cet usage)

- **Ne soyez pas administrateur**

Tout programme exécuté au sein d'un système Windows possède les droits de l'utilisateur qui l'a lancé. Si cet utilisateur dispose des droits d'administrateur, les programmes qu'il exécute auront donc également tous les droits sur le système.

C'est certes pratique pour réaliser des tâches de maintenance, mais catastrophique si l'administrateur exécute par mégarde un virus ou un cheval de Troie : le parasite aura alors tous les droits pour modifier le système !

Réservez donc le compte administrateur aux travaux qui nécessitent vraiment des droits étendus (installation de certains logiciels, mises à jour, etc.…) et créez-vous un compte utilisateur standard pour travailler au quotidien.

Attention : Certains logiciels mal conçus exigent des droits administrateurs pour fonctionner (et Windows ne facilite pas toujours les choses, n'ayant pas été conçu pour être un système multiutilisateurs).

Heureusement avec Windows 8 et les versions futures ce point sera un peu moins important puisque le véritable compte administrateur est désactivé par défaut.

- **Partitionnez votre disque dur**

Il est recommandé (mais pas obligatoire) de diviser le disque dur de votre PC en deux partitions qui se comporterons comme deux disque dur indépendants.

- Sur la première partition (C:\), qui fera environs un tiers de la taille totale du disque dur, il n'y aura que Windows et les programmes que vous utilisez.

- Sur la seconde partition (D:\), vous mettrez tout le reste, vos documents, les vidéos, les photos, la musiquent.

Cette configuration facilite le travail d'entretien du PC et la sauvegarde du système (Windows +programmes) comme celles des données.

De nombreux constructeurs vendent des PC installé d'origine avec 3 partitions, les deux que nous avons déjà vues, système et données, la troisième contient un programme et les informations pour réparer votre PC en cas de panne. Dans le pire des cas ce programme pourra remettre votre PC dansa configuration qu'il avait à sa première mise en route.

- **Clonez de la partition contenant Windows et les programmes**

Pour les utilisateurs avancés il existe des programmes comme **AOMEI Backupper** qui permettent de sauvegarder l'intégralité de Windows et des programmes que vous avez installés sur un disque dur extérieur. puis en cas de panne de mettre votre système dans l'état ou il était le jour de cette sauvegarde.

Depuis Windows 7 il est possible de réaliser une prouesse similaire en créant des points de sauvegarde. Cette solution reste plus simple a employer et fonctionne parfaitement bien sauf en cas de panne de votre disque dur.

- **Faites les mises à jour de sécurité de Windows**

Les mises à jour de Windows sont activées par défaut, si jamais vous les avez désactivées je vous recommande vivement de les réactiver et de choisir l'option « uniquement les mises à jour de sécurité »

- **Contrôlez de temps en temps votre sécurité**

Plusieurs services en ligne, souvent gratuits, vous permettent de savoir rapidement si votre ordinateur est accessible depuis l'internet. Ils testent en réalité votre pare-feu en essayant de déterminer le sports ouverts sur votre PC. Certains vont plus loin et tentent de repérer d'éventuels chevaux de Troie qui seraient déjà installés sur votre système (Symantec Security Check par exemple).

De nombreux éditeurs d'antivirus proposent également une analyse gratuite de votre disque dur directement depuis le réseau mondial. Vous en trouverez la liste sur le site http://www.inoculer.com.

Et vous pouvez vous-même vous assurer des points suivants

- Relisez de temps en temps les règles de bases de sécurité

- Contrôler périodiquement les mises à jour automatiques de l'antivirus
- Contrôler le bon fonctionnement des sauvegardes automatiques
- Faire de temps en temps l'entretient des disques durs de du PC (ce sera le sujet du chapitre « Fitness for Windows »)