Blinder son PC dès l'installation - 1/2

Spywares, virus, attaques, trojans, dialers. Comment éviter tout ça avant qu'il ne soit trop tard.

Nous avons tous été confrontés (si vous êtes parmi les 99% d'utilisateurs à utiliser Windows sur votre PC) à un moment ou à un autre à un virus informatique, un spyware (logiciel espion), un dialer (numéroteur téléphonique généralement vers des sites X) qui veut s'installer de force sur votre PC, ou d'autres joyeusetés.

Souvent quand le mal est fait, il est assez compliqué de s'en débarrasser, tant les procédures de suppression sont complexes et laborieuses (installation de logiciels type Ad-Aware, SpyBot, HiJackThis, j'en passe et des meilleurs...). Alors pour contrer tout ça, mieux vaut blinder le système d'exploitation dès le début, c'est à dire juste après l'installation de Windows !

Pour ça, 3 éléments sont nécéssaires : l'antivirus, le pare-feu (ou *firewall*) – ces deux élements sont à installer avant toute connexion à Internet - et un bon navigateur Internet.

L'antivirus

Il n'y a pas forcément besoin de devoir dépenser beaucoup pour avoir un anti-virus efficace et régulièrement mis à jour.
La gamme Norton est un peu trop lourde à mon goût, mais peut s'avérer valable non pas pour une utilisation permanente mais pour un check-up de temps en temps.

Après tout dépend de votre philosophie, de votre processeur et de votre porte-monnaie. Je vous conseillerai d'abord Panda Titanium : il est très efficace, se met à jour automatiquement avec les nouvelles signatures de virus mais son outil de protection permanente (pas besoin de scanner le PC toutes les heures, l'antivirus tourne en arrière plan) est assez gourmand en mémoire et en processeur. Il est gratuit 30 jours.

Celui que j'utilise : AVG Frée Edition. Totalement gratuit, lui aussi se met à jour automatiquement et possède également un outil de protection permanente. Mais se révèle assez boiteux quand il s'agit d'éliminer à proprement dit le virus. A réserver aux utilisateurs un minimum confirmés ou bien à des machines qui ne sont pas souvent infectées. Le truc qui tue : AVG regarde même dans vos mails et supprime les pièces jointes quand elles se révèlent être infectées ! Donc aucun risque, même avec Outlook Express (enfin c'est quand même suicidaire d'utiliser ce progamme pour ses mails =/)

Le pare-feu/firewall

Imaginez : votre PC est comme une chèvre qui allaite (si, si). Votre machine a ce qu'on appelle des ports, chaque port étant la plupart du temps dédiée à une application bien spécifique (port 21 pour le FTP – le transfert de fichiers -, port 80 pour le HTTP – consultation de pages Web -, etc...). Ces ports sont comparable aux pis de la chèvre. Malheureusement, comme sur la chèvre certains ports de votre PC sont ouverts et peuvent permettre à d'autres utilisateurs de joindre votre machine et essayer de la faire redémarrer ou bien essayer d'y placer un programme qui rapatriera par exemple des numéros de carte bancaire présents sur votre PC... (j'exagère à peine). Le rôle du pare-feu est de protéger ces ports pour que seuls les applications et les utilisateurs en qui vous faisez confiance y aient accès (imaginez qu'un chevreau aille prendre du lait sur une chèvre qui n'est pas sa mère... C'est n'importe quoi !).
Pour cela, c'est très simple, après l'installation du pare-feu, vous aurez à autoriser telle ou telle connexion (vers votre PC ou à partir de votre PC) au fur et à mesure. Par exemple, Internet Explorer, puis Kazaa, puis Outlook, puis RealPlayer, etc... (ne vous inquiétez pas, vous n'aurez à le faire qu'une seule fois )

Blinder son PC dès l'installation - 2/2

Des exemples de firewalls : ZoneAlarm (gratuit), Sygate Personal Firewall (celui que j'utilise, gratuit pendant 30 jours, il est tellement bien que je l'ai finalement acheté... environ 30 €, de mémoire).

Eviter les programmes trop lourds comme ceux de la gamme Norton qui vous protègent certes, mais ne vous font pas réellement comprendre le principe du pare-feu, tellement c'est simplifié.

Le navigateur

Cela fait maintenant quelque temps qu'Internet Explorer n'a plus été un minimum revisité : il laisse passer les popups (fenêtres s'ouvrant automatiquement), utilise encore l'ActiveX (technologie de contenu souvent utilisée à mauvais escient par certains sites Internet), fournit des patchs (corrections) de sécurité tardivement, n'est pas évolutif, bref c'est le navigateur à jeter. Tout comme Outlook Express, le client mail de la même trempe, ou c'est vraiment trop facile de se prendre un virus.

Pourquoi donc tout le monde l'utilise ? Tout simplement parce qu'il est présent de base sur tous les PC équipés de Windows.
Pourquoi est-ce que tout le monde continue à l'utiliser ? Tout simplement parce que tous les sites Internet sont prévus d'abord pour Internet Explorer. Il y en a même qui refusent l'accès à d'autres navigateurs, ceux là sont à mettre au bûcher.

L'alternative : **Mozilla Firefox**. C'est un navigateur GRATUIT, très simple, évolutif et gérant au moins autant de plug-ins (Flash, Visites 3D, etc...) qu'Internet Explorer, sauf l'ActiveX, ce qui vous évite de vous choper de mauvais petits logiciels qui font ch***. Il bloque les pop-ups automatiquement (vous pouvez toujours désactiver cette fonctionnalité). On peut lui appliquer des thèmes graphiques, lui ajouter un lecteur de blogs, etc... Plein de choses qui font de ce navigateur un outil remarquable.

D'autres éléments qui risquent de vous convaincre : http://frenchmozilla.org/firefox/pourquoi/
Il est disponible en français sur : http://frenchmozilla.org/firefox/

Pour ceux qui veulent encore utiliser Internet Explorer car certains sites ne prévoient pas que des Internautes puissent être assez intelligents pour choisir autre chose qu'IE comme navigateur... l'accessoire indispensable se révèle être la Google Toolbar, qui en plus d'être très pratique pour rechercher des infos plus rapidement, bloque également les pop-ups très efficacement.

Une alternative à Outlook Express, dans le même esprit : **Mozilla Thunderbird**, disponible ici : http://frenchmozilla.org/thunderbird/