Qu'est-ce qu'un internaute averti doit savoir ?

Il faut savoir qu'Internet, appelé aussi « **le monde virtuel** », représente les **mêmes dangers que dans le monde réel**, notre monde. En conséquence nous devons être vigilants et ne pas cliquer sur tout ce qui bouge et réfléchir avant de cliquer sur un lien proposé. Il faut sécuriser son ordinateur avec un antivirus et un firewall avec en complément un antispyware et surtout un antimalware qui comprend un **antitroyen, antibackdoor, antirootkit, antikeylogger, etc.**

En dehors de ces **protections obligatoires** il est **impératif** de faire les mises à jour du système d'exploitation (**Windows®, Mac® et Linux®**) **ainsi que les mises à jour de tout autre logiciel installé sur l'ordinateur (Adobe Acrobat Reader, Java, ITunes, QuickTime, Winamp, VLC Media Player, Media Player, Real Player, Messenger, Apache, MySQL, etc.). Ceci est devenu un « must » entre temps, vu que ces logiciels représentent de temps à autre des failles critiques qui permettraient à un cybercriminel de prendre le contrôle de la machine à l'insu de leur propriétaire, si elles ne sont colmatées. Nous vous invitons à suivre notre didacticiel qui vous guide à travers l'installation et l'utilisation du logiciel de chez SECUNIA :**

http://www.internetmonitor.lu/download/Scan_gratuit_de_logiciels_installes_15122006.pdf

Un Mac a d'ailleurs été hacké en deux (2) minutes dû à une faille non colmatée du navigateur Safari, à la conférence CanSecWest
http://www.macgeneration.com/unes/voir/127098/un-macbook-air-hacke-en-deux-minutes .

Évitez aussi de vous servir des plateformes d'échange de fichiers, appelées aussi **P2P** (**peer to peer**), ou disons plutôt de « **pire en pire** ». La plupart des fichiers à télécharger sont contaminés avec des malwares (troyens, spyware, etc.) et infectent ainsi votre ordinateur, sans parler de l'aspect de légalité, dépendant d'un pays à l'autre. Votre ordinateur sera transformé en « **PC zombie** » et téléguidé par les cybercriminels (à votre insu) pour effectuer des actions illégales, dont vous pouvez être tenus responsables...

N'utilisez pas de clés USB, lecteur MP3, Cds, DVDs, cartes Flash, disquettes sur l'ordinateur avant de les avoir scannés avec votre antivirus. Après avoir prêté votre clé USB et/ou utilisé votre clé USB dans un cyberespace (Internet Café), chez toute autre personne, supermarché et chez le marchand photo, scannez-la aussi avec votre antivirus et votre antimalware !!! Pas tout ordinateur public est assez sécurisé et peut être infecté, dont votre matériel en sera infecté aussi plus tard.

Ne téléchargez les logiciels gratuits que de sources bien connues et évitez les sites se terminant avec un « **z** » tels que « **warez, serialz, etc.** », ce sont des sites illégaux qui en plus sont contaminés avec des malwares.

Nous vous recommandons les sites Internet suivants pour télécharger des logiciels gratuits :

www.telecharger.fr

www.clubic.com

www.libellules.ch

www.chip.de

www.pcwelt.de

Il faut aussi savoir (réaliser) que :

- **Ce sont surtout les ordinateurs privés qui sont visés par les cybercriminels dû au fait que la plupart ne sont pas sécurisés et représentent ainsi une proie facile pour eux.**

Plus grand qu'il est le nombre d'ordinateurs sécurisés, moins grande sera l'influence et la présence des cybercriminels !!!

- **L'ordinateur est un outil technique et peut être vu comme notre moyen de transport pour le monde virtuel (Internet). Chaque moyen de transport a besoin de sécurité, de révisions et de soins techniques pour garantir notre sécurité et celle des autres !!!**

Ma recommandation :

Une proposition de configuration bien sécurisée « type » pour emploi domestique :

- **Une « suite de sécurité » comprenant un antivirus, un firewall et une protection antiphishing, telle que :**

Norton Internet Security 2008, Kaspersky, GDATA, Bit Defender, etc.

N.B.: La suite de sécurité Norton a l'avantage d'avoir intégré aussi une protection « antibotnet » (prochainement).

- **Un antimalware (antitroyen, antibackdoor, antikeylogger, antirootkit, etc.) tel que « a squared »** http://www.emsisoft.net/fr . Cet antimalware existe en version gratuite et en version payante. **Il a la particularité de lancer un processus de scan de mémoire avec un examen heuristique et non avec des signatures.** La version payante (+/- 29 €) a l'avantage d'avoir intégré une protection en temps réel.
- Un antispyware gratuit tel que «**Spybot search&Destroy** » http://www.safer-networking.org/fr/download/index.html et/ou « **Ad Aware** » http://www.lavasoft.com/

- Un logiciel de contrôle des mises à jour de tout logiciel installé sur l'ordinateur, tel que **SECUNIA** http://www.internetmonitor.lu/download/Scan_gratuit_de_logiciels_installes_15122006.pdf

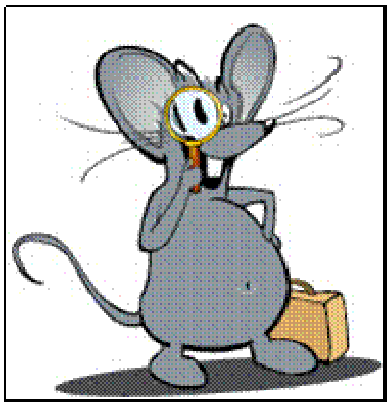
- Installez le logiciel gratuit « **McAfee Site Advisor** » qui s'intègrera dans votre navigateur (Internet Explorer et Firefox) et vous avertira des sites Internet douteux. : http://www.siteadvisor.com

Pourquoi une protection complémentaire à l'antivirus ?

Tous les antivirus n'arrivent plus à suivre l'évolution rapide des malware et représentent eux-mêmes déjà des risques, des failles de sécurité. Thierry ZOLLER et Sergio ALVAREZ, deux rechercheurs en sécurité ont prouvé ceci en pratique lors du HackLu2007 http://www.hack.lu **à Luxembourg en faisant un « proof of concept » (preuve de concept). Ils ont dévoilé qu'il existe plus que 800 vulnérabilités documentées sur tous les produits antivirus présents au marché, lesquelles ont bien évidemment été signalées aux fabricants : lien en allemand** http://www.computerwoche.de/knowledge_center/it_security/1848636/index.html

Les cybercriminels (mafia informatique) sont dorénavant capables de paralyser les protections antivirus s'ils veulent.

Donc, sachant de ce qui est déjà possible à contourner, munissons-nous avec des protections supplémentaires, telles que décrites ci-dessus. Plus grand qu'il est le nombre d'ordinateurs sécurisés, moins grande sera l'influence et la présence des cybercriminels. Agissons pour le bien de nous-mêmes et de celui de la communauté !!!



N'oubliez pas non plus de rester informés sur les nouvelles vulnérabilités qu'il faudra ensuite colmater en téléchargeant les correctifs (updates/patches) proposés.

Pour être toujours bien informé, nous vous proposons de vous abonner à notre lettre d'information (Newsletter). Il suffit de vous connecter au site Internet http://www.internetmonitor.lu et naviguer sur le côté droit du site. Vous verrez un champ de texte dans lequel il vous faut inscrire votre adresse email, suivi d'un clic sur « OK ». Vous serez abonnés et vous recevrez notre lettre d'information gratuite toutes les deux semaines.

Vous avez même la possibilité d'être averti par GSM (Handy, Bluetooth, etc.) en tapant l'adresse URL : http://m.internetmonitor.lu/ .

Même que nous avons créé aussi une barre d'outils (Tool bar) spéciale de l'Internet Monitor qui s'intègre dans votre navigateur (Internet Explorer et Firefox), que vous pouvez télécharger à l'adresse URL : http://internetmonitorlu.ourtoolbar.com/.

Et « last but not least », recevez aussi nos informations RSS à l'adresse URL :

http://www.internetmonitor.lu/xml/syndication.rss.