SECURITY MONITOR

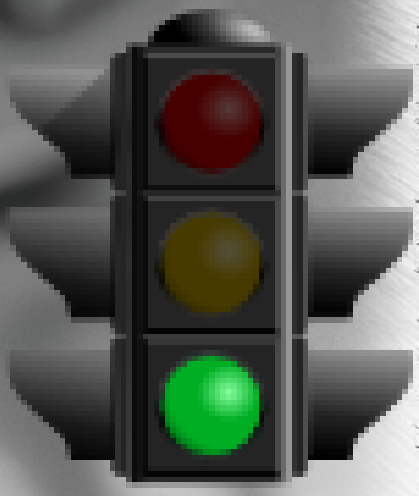
PC Sécurité

Numéro 2/MAI 2008

MGX GS MGX GS

w w w . ? ? ?

L‘ordinateur bien sécurisé



- Un regard critique sur le comportement sur Internet
- Tous les systèmes d‘exploitation sont vulnérables !!!
- Notre choix d’outils de sécurité gratuits
- Les outils de contrôle de la sécurité

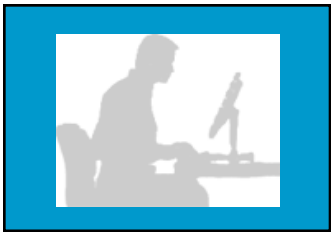
MGX GS 123456789#@

http://www.internetmonitor.lu
http://www.mysecureit.lu
http://www.cases.lu
http://www.lusi.lu

Sécurité PC & Internet.

Internet ⟹ Sécurité

Les ordinateurs sont présents maintenant dans presque tous les ménages et Internet fait partie de la vie quotidienne. En employant Internet nous naviguons dans la vie virtuelle, nous faisons partie d'une communauté ! Or, cette communauté ne peut vivre sans problèmes de sécurité que si tout individu a bien sécurisé son ordinateur (Mac et Linux y compris) !!! Voici nos conseils pour que cette merveilleuse communauté puisse continuer à exister en toute sécurité et prospérité.



Glossaire :

Malware:
Mot regroupant toute sorte de code malicieux.
Firewall :
Appelé aussi „**pare-feu**" est le portier de l'ordinateur qui gère le trafic entrant et sortant des données informatiques. Il contrôle les ports de l'ordinateur, il y en a 65.535 ports.
Troyen, trojan, cheval de Troie :
Programme malicieux qui en renferme minimum un autre programme malicieux.
Spyware :
Petits programmes qui s'installent sur votre ordinateur à votre insu et qui espionnent vos habitudes de surf. Ainsi vos habitudes seront envoyées envers le programmateur qui lui vous bombardera avec des fenêtres „pop-up" (fenêtres intempestives) contenant de la publicité ciblée !
Dialer :
Un dialer est un programme malicieux que vous pouvez attraper en téléchargeant des logiciels sur des plateformes douteuses. En principe un dialer ne peut être attrapé qu'avec un modem analogique. **Mais attention, avec le VoIP (Skype, etc.) il a été démontré qu'il est aussi possible d'attraper un dialer avec une connexion haut débit (adsl) !**
Un dialer est une connexion surtaxée et peut vous coûter très cher (50 €/clic, etc.) !

De même les ordinateurs sont de plus en plus utilisés dans les écoles comme outil pédagogique. Internet est devenu un outil précieux dont nous ne pourrons plus nous passer dans le futur, mais internet est aussi une source qui contient beaucoup de risques ; des risques qu'il faut éviter et aussi savoir les gérer, tels que :

- Le „**phishing**".
- Les „**spyware**".
- Les „**virus**".
- Les „**Troyens, chevaux de Troie, trojans**".
- Les „**malware**", en général (**backdoor**, **keylogger**, **troyen**, **dialer**, etc.)
- Les „**dialer**" ou connexion surtaxée.
- Le „**Cross-Site-Scripting**" (**XSS**), ou attaque virale en visitant un site Internet.

Mais en respectant quelques règles nous pouvons surfer avec un maximum de sécurité, dont voici nos conseils :

- **Installez un „antivirus"** et faites quotidiennement les mises à jour (**updates / live update**) de celui-ci.
- **Installez un „pare-feu"** (**firewall**), de préférence un autre que celui de **MICROSOFT® XP**. Celui de **MICROSOFT® XP** ne contrôle que le trafic entrant et pas le trafic sortant.
- **Installez un „antispyware",** de préférence deux pour une meilleure performance. Nous vous conseillons „**Spybot Search & Destroy**" et „**Ad Aware**".
- Installez un „**antimalware**" (**antitroyen, antirootkit, antibackdoor, antikeylogger, antidialer, etc**.), tel que „**a squared**" **www.emsisoft.net/fr.**
- **Téléchargez régulièrement** les mises à jour (**updates / patches**) de **MICROSOFT®,** mais aussi de **MAC®** et **de LINUX®** (nul n'est parfait) ! Ceci est un „**must**", contrairement à ce que la plupart des gens croient !
- **Veillez à télécharger régulièrement les mises à jour (updates) de tout autres logiciels installés sur votre ordinateur.**
- **N'ouvrez jamais** de courrier électronique de personnes inconnues et surtout pas les pièces jointes (attachments)!
- **Ne répondez jamais** à des courriers électroniques venant d'institutions bancaires, **eBay** et d'autres institutions. Il y a danger de „**phishing**", appelé encore „**hameçonnage par courrier électronique**" !
- Ne téléchargez pas de la musique, vidéos et logiciels illégaux sur des plateformes d'échange de fichiers (P2P/peer to peer), car la majorité de ces fichiers téléchargés sont infectés de malware !!!

Restez informés sur les dernières informations de sécurité, soit par abonnement à des Newsletter (lettre d'informations) et/ou en lisant des magazines PC et en suivant les articles de presse sur l'informatique dans vos journaux quotidiens !

En respectant ces quelques règles mentionnées ci-dessus vous pouvez surfer en toute tranquillité ! Mais veuillez remarquer quand même qu'une sécurité à 100% n'existe pas et est illusoire ! Le maillon le plus faible est et restera toujours l'être humain (nobody is perfect / nul n'est parfait) !

„Les règles d'or pour avoir un ordinateur sécurisé“

SOUS WINDOWS® XP/

Une sécurité à 100% n'existe pas et est illusoire ! Néanmoins nous pouvons nous protéger au maximum avec un minimum d'investissement.

Ce qu'il faut savoir en première instance :

En dehors des outils de protection il faut encore respecter certains autres critères, choses dont la plupart des gens n'y pensent pas. Un ordinateur, pour bien fonctionner d'une manière stable, nécessite au moins 30% d'espace libre sur le disque dur. Ce n'est pas seulement la mémoire vive (RAM) dont Windows® a besoin, mais Windows® utilise aussi le disque dur (hard disk) comme mémoire tampon pour stocker temporairement des données.

Au cas où il y aurait moins de 30% d'espace de libre il faut envisager de faire de la place sur le disque dur. Téléchargez et installez le logiciel „**CCleaner**“, dont voici un lien pour télécharger le didacticiel, qui vous guidera à travers l'installation et l'utilisation

http://www.internetmonitor.lu/download/ccleaner_27082006.pdf

„**CCleaner** (**Crap Cleaner**)“ enlève les fichiers **temporaires**, les **fichiers Internet temporaires**, le **fichier** „**index.dat**“ et il nettoie la **base de registre**. De ce fait, il y aura beaucoup de chance que vous arriveriez au dessus des **30% d'espace libre**.

Si tel ne serait pas le cas, il faudrait ouvrir le panneau de contrôle et par „**Ajout/Supprimer**“ supprimer des programmes afin de libérer de la place.

Aussi faut-il de temps à autre veiller à faire une **défragmentation du disque dur**. Ceci augmente aussi la rapidité d'accès aux données.

Un didacticiel complet, vous guidant à travers l'utilisation de la défragmentation peut être téléchargé à l'adresse :

http://www.internetmonitor.lu/download/Defragmentation du disque dur avec decoupe.pdf

Les outils de protection peuvent seulement fonctionner au maximum quand le système d'exploitation dispose d'assez de ressources. Autrement les outils de protection seront freinés et n'arrivent pas à détecter les infections virales et infections de malware !

Primordial et obligatoire est aussi le téléchargement des mises à jour de Windows® , ainsi que le téléchargement des mises à jour des logiciels indispensables (Macromedia Flash®, Adobe Acrobat Reader®, Java®, QuickTime®, ITunes®, VLC Media Player, Open Office, Firefox, etc.).

Mises à jour Windows® :

http://update.microsoft.com

Vérification des mises à jour d'autres logiciels :

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

Pratique „Sécurité PC&Internet“ :

http://www.internetmonitor.lu/download/Pratique_Securite_PC_Internet_27.06.2006.pdf

Vade-mecum de la sécurité :

http://www.internetmonitor.lu/download/Vade-mecum_Securite_PC_Internet_.pdf

UN REGARD CRITIQUE SUR INTERNET

L’œil critique, un regard critique sur Internet

L’année 2007 a montrée que les créateurs de code malicieux ne travaillent plus seul, mais qu’ils opèrent en groupe, on peut parler entre-temps **d’une mafia informatique qui est très bien organisée, qui travaille d’une manière professionnelle.** Ce ne sont plus les **script kiddies** (des jeunes et adolescents qui cherchent à se profiler et à devenir célèbres), pourtant ils existent encore, mais c’est la **mafia informatique** qui a trouvé le moyen le plus simple et presque sans risques de **gagner illégalement de l’argent** en créant du **code malicieux** pour **infecter les ordinateurs**.

Mais comment gagner de l’argent avec un ordinateur infecté ?

Les ordinateurs infectés avec du code malicieux (**virus**, **troyen**, **backdoor**, **keylogger**, **dialer**, etc.), appelés aussi **PC zombies**, **sont téléguidés** par les créateurs du code malicieux et **intégrés dans un réseau** (appelé aussi un **botnet**) qui peut comprendre des **dizaines de milliers d’ordinateurs, voir même 500.000 ordinateurs infectés et plus :**

http://www.internetmonitor.lu/index.php?action=article&numero=1030

Ce réseau (**botnet**) est utilisé pour :

- Envoyer du courrier non sollicité (**spam**).
- Faire des attaques contre des sites Internet pour les infecter et/ou pour bloquer leur présence sur Internet.
- Faire du chantage avec des données volées sur le (s) serveur (s) de firmes et demander une rançon pour pouvoir récupérer les données confidentielles.
- Faire l’échange de fichiers avec du matériel audio, vidéo et pornographique, voir même du matériel pédophile.
- Infecter de nouveaux ordinateurs pour agrandir le réseau botnet.

Les risques et dangers

L’échange de fichiers (P2P) :

L’échange de fichiers, appelé aussi le « **peer to peer** » (**P2P**), ou disons plutôt **de pire en pire** est une application qui est sous estimée en ce qui concerne l’état de sécurité de celle-ci. Ce que la plupart des internautes ne savent pas, c’est qu’en téléchargeant sur les plates-formes de P2P des pièces de musique, de films, logiciels, etc., ils téléchargent aussi des malware (troyens, virus, vers, etc.) à leur insu, comme petit bonus.

Il a été démontré que « Kazaa » est une plate-forme à haut risque :

Kazaa : 45% des fichiers exécutables seraient infectés. Si vous téléchargez des logiciels ou des jeux vidéo de Kazaa, vous pourriez obtenir plus que vous n'en demandiez puisque près de la moitié des fichiers exécutables seraient infectés par des virus, vers informatiques ou chevaux de Troie.
http://www.internetmonitor.lu/index.php?action=article&numero=155

D’autres plates-formes ne sont guères différentes !!!

„Les risques et dangers“

UN REGARD CRITIQUE SUR INTERNET

Le « Drive-by download »

Mais c'est quoi « Drive-by-Download » ?

Le **Drive-by-Download** n'est rien d'autre qu'une infection attrapée en visitant un site Internet préparé pour infecter votre ordinateur.

Quand votre ordinateur n'est pas suffisamment sécurisé, vous êtes vulnérables à toutes sortes d'infections !!!

Rappelons que ces attaques ne visent pas seulement les ordinateurs Windows ® !!! Chaque ordinateur (**Windows, Mac, Linux, etc.**) est équipé d'office, ou nécessitera tôt ou tard, ce que l'on appelle les **utilitaires indispensables**. Ces **utilitaires indispensables**, tels que **Adobe Acrobat Reader, Java, Firefox, Internet Explorer, Opera, Flash Player, Winzip, QuickTime, ITunes, etc.** ne sont pas sécuritaires !!! Dans des intervalles réguliers les experts de sécurité informatique trouvent des **failles (vulnérabilités) critiques**.

Ces **vulnérabilités critiques** permettent **d'injecter du code** (**code injection**) malicieux quand ces utilitaires ne sont pas mis à jour. Comme ces « utilitaires » sont indépendants du système d'exploitation (O.S.), tout ordinateur (Windows, Mac, Linux, et autres) peut devenir la proie (ou l'est déjà) de ces attaques, appelés **Cross site scripting** (**XSS**) !!!

En principe, vous êtes incités, par l'intermédiaire d'un courriel (courrier électronique, émail) ou par proposition d'un lien (link) dans un forum, à visiter un site Internet préparé. **Ce site Internet, ceci peut être un site Internet tout à fait normal (mais non-sécurisé), vous injectera du code malicieux (code injection) dans votre ordinateur.**

Ce code malicieux, connu aussi sous le nom de « **cross site scripting** » (**XSS**), contient des troyens (**chevaux de Troie, trojans**)
, qui quant à eux renferment des « **keylogger** » (enregistreurs de frappe) et des « **backdoor** » (**portes dérobées**). Ceci rend possible que votre ordinateur soit infecté et téléguidé (à votre insu) par la mafia informatique et il fera part d'un **botnet**, d'un réseau d'ordinateurs (**PC zombies**) téléguidés pour faire des actions illégales.

Lien : http://www.emsisoft.net/fr/info/a2/

Même que ceci se passe à votre insu, sachez que vous en êtes responsables de ces actions illégales devant la loi, en tout cas en ce qui concerne le Luxembourg !!!

Ce que dit le « Code Civil Napoléon » Luxembourgeois :

„Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence“. Dans d'autres pays il y a certainement des lois semblables.

Les lois luxembourgeoises (01.05.2008) :

http://www.cases.public.lu/fr/actualites/actualites/2007/03/26_SID/Pierre-Beausse_Criminalite.pdf

http://www.vocats.com/index.php?id=169&L=1

„Les règles d'or pour avoir un ordinateur sécurisé“

L'ORDINATEUR BIEN PROTÉGÉ/!

Les outils de protection :

De nos jours il est nécessaire d'avoir installé les protections suivantes :

- **Un antivirus gratuit ou payant.**
- **Un firewall (pare-feu).**
- **Un antispyware, de préférence deux qui se complètent (Spybot Search&Destroy et Ad Aware).**
- **Un antimalware (antitroyen, antidialer, antikeylogger, antirootkit, etc.), tel que „a squared“.**
- **Un logiciel de détection des sites Internet frauduleux (McAfee Site Advisor).**

Avec cette combinaison de logiciels installés, vous êtes sécurisés au maximum (octobre 2007).

Liste des logiciels antivirus gratuits :

http://www.inoculer.com/gratuits.php3

Liste des suites de sécurité (antivirus+firewall+antispyware, etc.) :

http://www.01net.com/article/345998.html

Les antispyware gratuits :

Ad Aware :

http://www.pcentraide.com/index.php?showtopic=188

Spybot Search&Destroy :

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

L'antimalware par excellence „a squared“ :

http://www.emsisoft.net/fr

Détection de sites Internet frauduleux :

http://www.siteadvisor.com

Remarques :

Veuillez trouver ci-dessous une liste de logiciels pour ceux qui aiment des **protections supplémentaires (seulement pour utilisateurs avertis)** :

- **Super Antispyware** : http://www.superantispyware.com/
- **Advanced Microsoft Care** : http://www.iobit.com
- **Browser Hijack Retaliator :** http://www.zamaansoft.com/products/bhr/
- **BHO Demon :** http://www.majorgeeks.com/download3550.html

Mais n'oublions pas non plus le maillon faible dans la chaîne de la sécurité, l'être humain (nous) !!!

Avant tout c'est nous qui utilisons l'ordinateur et c'est bien nous qui surfons sur Internet par l'intermédiaire de l'ordinateur. L'ordinateur peut être vu comme le moyen de transport pour naviguer dans le monde virtuel (Internet).

Par conséquent le conducteur d'un moyen de transport, **un être humain, n'est pas toujours attentif et court des risques ! L'être humain n'est pas parfait, loin de là !!!**

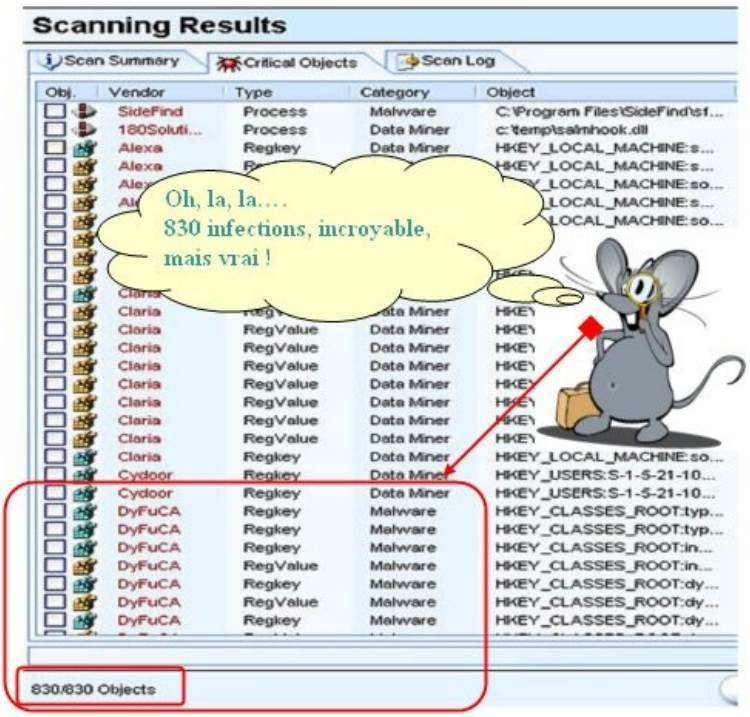
Veuillez télécharger mon didacticiel „**Sécurité PC&Internet**“ qui vous expliquera en détail **les démarches à ne pas faire :**

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

LES RISQUES D'UN ORDINATEUR NON PROTÉGÉ

POURQUOI ÊTRE PROTÉGÉ ?

PC infecté d'un jeune garçon de 13 ans



20 troyens, 25 browser hijacker, 15 virus, le reste sont des spyware...
3 jours d'interventions pour décontaminer l'ordinateur !

Un antivirus + firewall + antispyware sont indispensables !

Un ordinateur non protégé ne présente pas seulement un risque pour son propriétaire, mais aussi un risque pour la communauté (nous tous) !!!

Toutes copies faites sur un médium de sauvegarde (appareil photo digital, CD, DVD, cartes flash, clé USB, Memory Card, etc.) par l'intermédiaire d'un ordinateur infecté, infectent aussi un autre ordinateur dès quelles sont utilisées par celui-ci.

Un ordinateur infecté et qui est connecté à Internet distribue son (ses) infection (s) aux autres ordinateurs non sécurisées connectés à Internet !!!

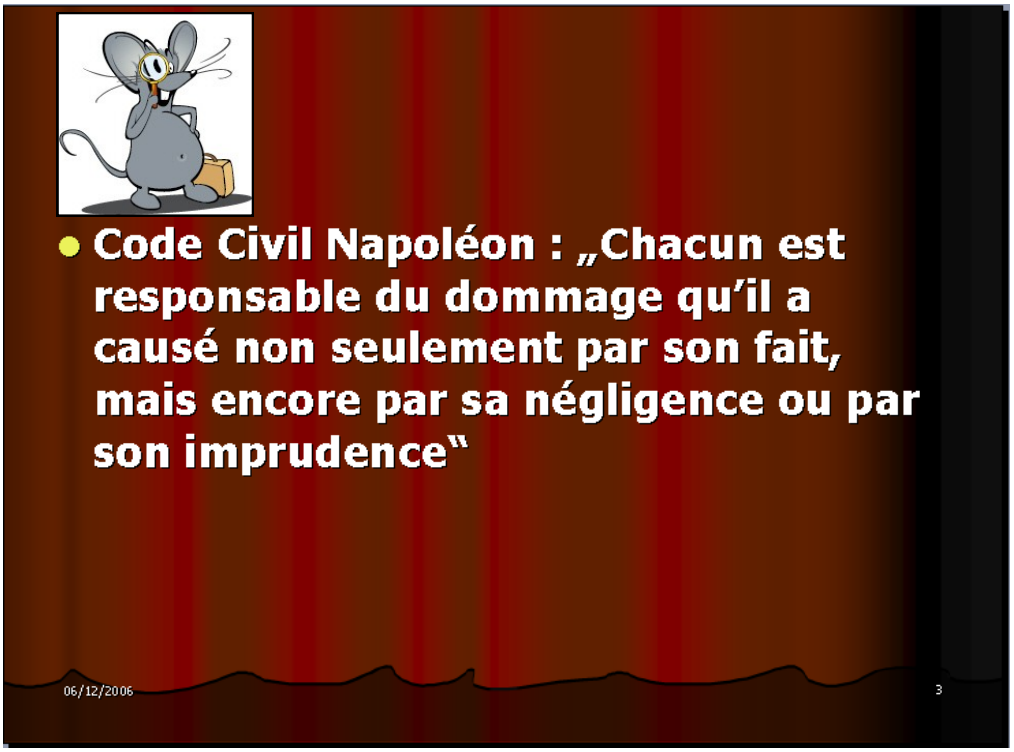
Un ordinateur non sécurisé est une proie facile pour la mafia informatique. Ces truands utilisent les ordinateurs non sécurisés et les transforment en „PC zombie", des ordinateurs téléguidés à l'insu de leurs propriétaires !!!

Même que ces ordinateurs zombies sont raccordés ensemble en réseau (botnet) pour faire des attaques massives contre des sites Internet !!! Soit que c'est pour faire des attaques du type „DDOS" afin de bloquer un site Internet (gouvernements, sites commerciaux, police, sites Internet de sécurité, etc.) pour qu'il ne soit plus présent sur Internet et/ou pour préparer des attaques contre les serveurs principaux qui font fonctionner Internet, ceci dans le but pour „éteindre" Internet !!! Des attaques similaires avaient déjà réussi à bloquer 3 sur 11 serveurs principaux d'Internet .

Un ordinateur infecté infecte aussi les autres ordinateurs et si les ordinateurs sont infectés par un Troyen (cheval de Troie, trojan) alors ils recherchent automatiquement d'autres ordinateurs infectés pour les intégrer dans un réseau (botnet) qui à lui sera contrôlé par ses programmeurs pour faire des actions illégales. Et ce sont les propriétaires des ordinateurs qui en sont responsables envers la loi, même en étant inconscients du problème !!!

LES RISQUES D'UN ORDINATEUR NON PROTÉGÉ

CE QUE DIT LA LOI LUXEMBOURGEOISE !



Cette phrase explique vraiment tout et elle est aussi valable pour Internet !!!

Les autres lois sur les TIC au Luxembourg :

http://www.cases.public.lu/fr/actualites/actualites/2007/03/26_SID/Pierre-Beausse_Criminalite.pdf

http://www.vocats.com/index.php?id=169&L=1

Les lois chez nos voisins :

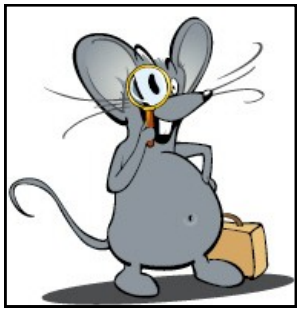
Droit du net (France) :

http://www.droitdunet.fr

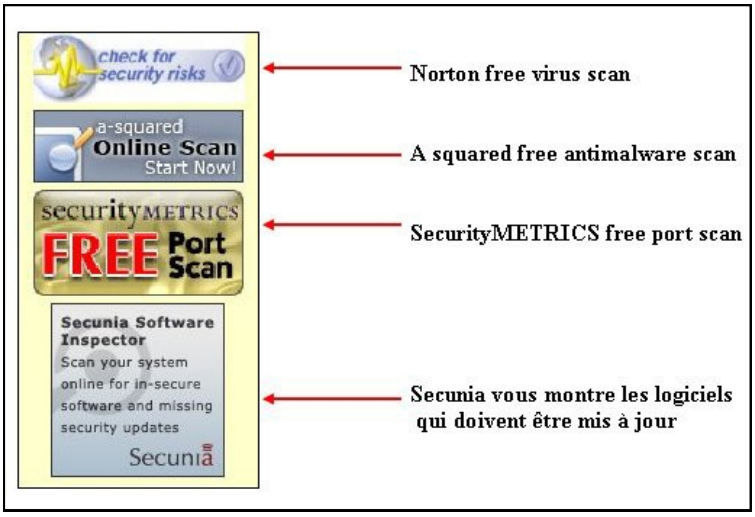
Contrôle de la sécurité

L'ORDINATEUR BIEN PROTÉGÉ/

Est-ce que mon ordinateur est bien sécurisé ?



Certainement vous vous êtes déjà posé cette question, mais comment savoir ?
Et pourtant ce n'est pas si difficile que ça. « **Internet Monitor** » **http://www.internetmonitor.lu vous offre gratuitement des services en ligne pour tester la vulnérabilité de votre ordinateur.**



En dehors de la possibilité de contrôler la sécurité de l'ordinateur en ligne (online) il existe aussi des logiciels gratuits qu'il faut installer sur l'ordinateur pour faire certains tests.

La sélection de „l'Internet Monitor" (freeware) :

Microsoft Baseline Security Analyzer 2 :

http://www.microsoft.com/france/securite/outils/mbsa.aspx

Belarc System Advisor :

http://www.belarc.com/free_download.html

Sophos Anti Rootkit :

http://www.sophos.com

Internet Monitor tool bar

„**L'Internet Monitor**" vous propose aussi le téléchargement et l'utilisation gratuite de sa **barre d'outils** (**tool bar**) qui contient des liens envers des didacticiels de sécurité, etc.

LISTE DE LIENS POINTANT ENVERS :

des sites francophones se consacrant à la sécurité PC&Internet, des sites d'entraide PC, des sites de vulgarisation informatique

RSS FEEDS :

Les fils RSS de l'Internet Monitor sont installés d'office

LA SECTION "FREEWARE" :

Profitez, des meilleurs logiciels pour décontaminer votre ordinateur au cas d'une infection virale, des astuces pour le dépannage de votre ordinateur, des tutoriaux informatique---> L'ordinateur transparent et facile à manier !!!

MOTEUR DE RECHERCHE :

Le moteur de recherche de Google (FR) est installé d'office.

EMAIL NOTIFIER :

Un notificateur de courriel (émail) est installé, lequel vous configurez avec votre compte de messagerie, afin d'être notifié automatiquement de nouveaux courriers (paramétrable) !

Pour télécharger cette barre, qui d'ailleurs est munie d'une fonction de désinstallation, cliquez ici svp :

http://internetmonitorlu.ourtoolbar.com

NOTEZ QUE LA TOOLBAR EST GRATUITE ET QU'ELLE NE CONTIENT AUCUN ADWARE, SPYWARE OU AUTRE CHOSE DE MALVEILLANT !!!

La sécurité bien appliquée !!!

L'ORDINATEUR BIEN PROTÉGÉ

Récapitulatif :

En principe, n'importe quel antivirus que vous choisissez est bon. **Il y en a qui sont meilleurs que certains, mais le principal est que vous soyez protégés par l'installation d'un antivirus (gratuit ou payant). Mais, pas plus qu'un seul !!!**

Et n'oubliez pas non plus svp, qu'il vous faut aussi un firewall (pare-feu) !!!----> obligatoire !!! Mais, pas plus qu'un seul !!!

Un antivirus vous protège principalement contre les virus et parfois aussi contre certains spyware, mais ce n'est pas son rôle principal.

Il vous faut des protections supplémentaires contre les spyware et aussi contre les troyens.

À recommander sont :

1.) **Antispywares** : deux qui se complètent, soit "**Spybot Search&Destroy**" et "**Ad Aware**"

2.) Un **antimalware** (**antitroyen, antirootkit, antikeylogger, antidialer, etc**.) tel que "**a squared**".

3.) **Faire régulièrement les mises à jour de Windows.**

4.) **Faire régulièrement les mises à jour des autres logiciels installés sur votre ordinateur.**

Je vous invite à suivre les didacticiels suivants, qui vous expliqueront en détail comment installer et utiliser les logiciels mentionnés (langage compréhensible, pas trop technique) :

L'ordinateur bien protégé :

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

Scan gratuit des logiciels installés :

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

L'ordinateur non-sécurisé :
http://www.internetmonitor.lu/download/risques_pc_non_protege.pdf

Pour savoir si un site Internet visité est dangereux et s'il contient du contenu **malicieux**, téléchargez „**McAfee Site Advisor**" à l'adresse URL :

http://www.siteadvisor.com/

Si cela vous intéresse à savoir plus, je vous invite à visiter les sites suivants :

MySecureIT (gratuit) :

http://www.mysecureit.lu/

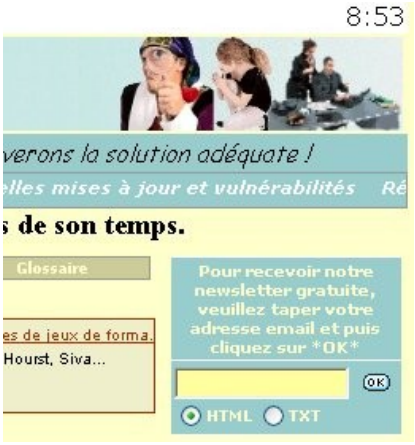
École virtuelle (e-Learning) sur la sécurité PC&Internet (gratuit) :

http://www.ecolevirtuelle-pcsecurite.com

Au bon plaisir d'apprendre, de devenir vigilant et de ce fait, sans problèmes sur l'ordinateur !!!

En dehors des malware discutés il existe aussi encore les vulnérabilités. Une vulnérabilité est une faille de sécurité d'un **système d'exploitation** (**OS**) et/ou d'un **programme** et/ou **logiciel**. Afin d'être toujours au courant des nouvelles **vulnérabilités**, veuillez vous inscrire au **Newsletter** (**lettre d'information**) de notre „**Internet Monitor**" à l'adresse :

http://www.internetmonitor.lu.



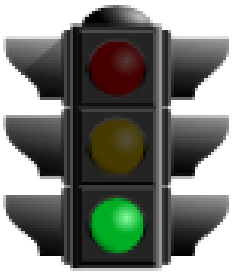
Conseils de sécurité et savoir-faire

L'ORDINATEUR BIEN PROTÉGÉ ET SÉCURITÉ APPLIQUÉE

Afin de savoir comment utiliser nos conseils et de programmer hebdomadairement les mises à jour, ainsi que de s'occuper de l'entretien de l'ordinateur, je vous invite à télécharger le didacticiel suivant, qui vous propose aussi des feuilles EXCEL avec les dates préprogrammées.

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

La sécurité ne se discute pas, elle s'applique !!!



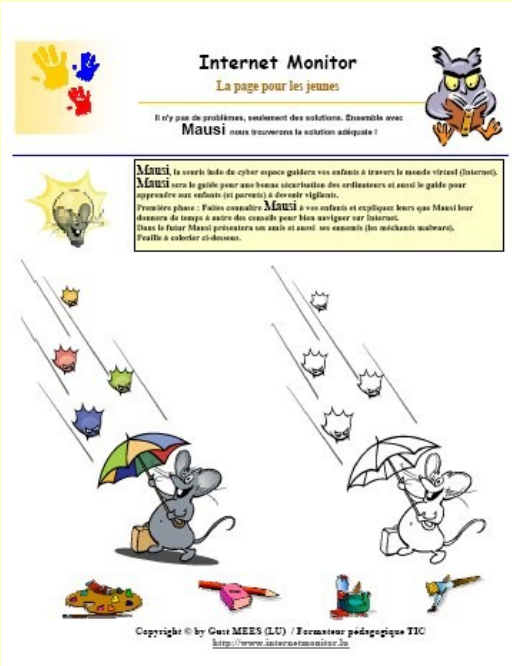
Pour vous aider à comprendre certains mots techniques :

http://www.emsisoft.fr/fr/kb/articles/tec080424/

http://fr.wikipedia.org/wiki/Accueil

Pensez à vos enfants, apprenez à vous servir d'une manière sécurisée d'Internet et puis transmettez-leurs votre savoir !!! Assumez votre responsabilité !

Dès le jeune âge apprenez-leurs la sécurité !!!



Conseils de sécurité, savoir-faire et information

L'ORDINATEUR BIEN PROTÉGÉ ET SÉCURITÉ APPLIQUÉE

Récapitulatif :

De nos jours il est nécessaire d'avoir installé les protections suivantes :

- **Un antivirus gratuit ou payant.**
- **Un firewall (pare-feu).**
- **Un antispyware, de préférence deux qui se complètent (Spybot Search&Destroy et Ad Aware).**
- **Un antimalware (antitroyen, antidialer, antikeylogger, antirootkit, etc.), tel que „a squared".**
- **Un logiciel de détection des sites Internet frauduleux (McAfee Site Advisor).**
- **Il est primordial de télécharger et installer les mises à jour des systèmes d'exploitation (Windows, Mac et Linux inclus) !!! Ils sont nécessaires pour la sécurité de l'ordinateur !!!**
- **Il est primordial de télécharger et installer les mises à jour des autres logiciels présents sur l'ordinateur !!! Ils sont nécessaires pour la sécurité de l'ordinateur !!!**

Quand notre ordinateur est sécurisé nous assurons aussi la sécurité de la communauté !!! Quand notre ordinateur est infecté, nous infectons aussi la communauté !!! Internet nous rappelle les principes fondamentaux d'une société. Une société ne peut vivre sans problèmes et ne peut être sécurisée, que si l'individu en soi-même respecte les règles de la société (communauté) !!!

Par conséquence, chacun est responsable du bon fonctionnement de la communauté, Internet y compris !!!

Comment rester informer ?

Internet Monitor www.internetmonitor.lu est un magazine qui se consacre à la sécurité domestique des ordinateurs et à la protection des enfants. **Internet Monitor offre des didacticiels pédagogiques** qui peuvent être téléchargés **gratuitement**, des **outils gratuits de contrôle de la sécurité** et un **newsletter**, ainsi que des **vidéos pédagogiques**.

Internet Monitor offre aussi la syndication de contenu, appelé aussi des « **Fils RSS** », simple à intégrer dans chaque site Internet et à lire avec un « **RSS Reader** » au format « **RSS** » et « **Atom** ». L'abonnement gratuit peut se faire ici www.internetmonitor.lu/xml/syndication.rss.Il vous est aussi possible de **lire les « Fils RSS » (nouveautés de la sécurité) sur votre cellulaire (Handy, GSM, Bluetooth) à l'adresse suivante :** http://www.internetmonitor.lu/m.

Toolbar gratuite : http://internetmonitorlu.ourtoolbar.com/ .

Abonnez-vous gratuitement aux fiches de sécurité informatique de mySchool!

En collaboration avec l'Internet Monitor (http://www.internetmonitor.lu), site internet édité par M. Gust MEES, formateur pédagogique TIC (Gérant de l'Internetstuff ETTELBRUCK) et mySecureIT, *mySchool!* publie **52 fiches sur la sécurité informatique**. Ces fiches sont formulées de manière très simple avec un jargon technique limité au plus strict minimum afin que tout le monde puisse les comprendre aisément et en tirer un bénéfice maximal. Des liens vers des sites qui vous faciliteront la vie et beaucoup de captures d'écran qui rendent les explications encore plus claires vous feront adorer ces fiches. Réalisées plutôt pour des débutants que pour des pros en informatique, même ces derniers peuvent encore glaner l'une ou l'autre information précieuse.

C'est gratuit! Inscrivez-vous une seule fois ci-dessous et vous recevrez chaque semaine une des 52 fiches de sécurité.

... et une cure de wellness... pour votre ordinateur! Parmi toutes les personnes qui se sont abonnées à ce site, **10 personnes bénéficieront d'un check-up total de sécurité gratuit de leur ordinateur**. Ce check-up, offert gracieusement par l'Internet Monitor, vous permettra de faire vérifier tous les logiciels de votre ordinateur pour contrôler s'ils ne sont pas affectés par des virus, chevaux de Troie, spyware ou malware. Il va de soi que ces problèmes, une fois identifiés, seront éliminés par les spécialistes de l'Internet Monitor.

La sécurité informatique nous concerne tous! Agissons!

Veuillez aussi vous abonner à nos cours pédagogiques gratuits au site Internet du Ministère de l'Éducation nationale « MySecureIT » : http://www.mysecureit.lu.

Et profitez aussi de notre école virtuelle (e-Learning) gratuite sur la sécurité PC&Internet à l'adresse :

www.ecolevirtuelle-pcsecurite.com

Mieux vaut prévoir que guérir !!!

LES OUTILS DE PROTECTION GRATUITS

L'ORDINATEUR BIEN PROTÉGÉ ET SÉCURITÉ APPLIQUÉE

L'antimalware « a squared » :

Lien de téléchargement : http://download4.emsisoft.com/a2FreeSetup.exe

La vidéo de démonstration : http://www.emsisoft.fr/en/info/a2/scanner/

Browser Hijack Retaliator (BHR)

« BHR » est un utilitaire qui vous protège contre le « browser hijacking », le détournement de votre navigateur. La mafia informatique devient de plus en plus malin pour gagner le maximum d'argent et de se fait elle invente toujours de nouveaux trucs pour piéger les internautes. Le détournement du navigateur en fait partie, le truc consiste à changer la page de démarrage du navigateur envers une page qui contient du code malicieux pour infecter l'ordinateur !!!

Au prochain démarrage de votre ordinateur, votre page de démarrage habituelle ne s'ouvre plus, mais en revanche vous seriez redirigés envers une page Internet qui contient du code malicieux afin d'infecter votre ordinateur et de faire de de celui-ci un « PC zombie », un ordinateur téléguidé qui sera intégré dans un botnet (réseau d'ordinateurs infectés et téléguidés pour faire des actions illégales) !!! Le truc consiste à changer le fichier « host », fichier qui ne devrait contenir qu'une seule entrée, l'entrée « 127.0.0.1 localhost ». La mafia informatique change ce fichier et ajoute plusieurs entrées, qui vous dirigent automatiquement envers des sites Internet a contenu douteux. Veuillez télécharger et lire notre didacticiel, qui vous aide à éclairer votre lumière à l'adresse URL :

http://www.internetmonitor.lu/download/hostfile_hijacking_05042007.pdf

Le didacticiel contient aussi le mode d'emploi pour installer le « **BHR** ».

LES OUTILS DE PROTECTION GRATUITS

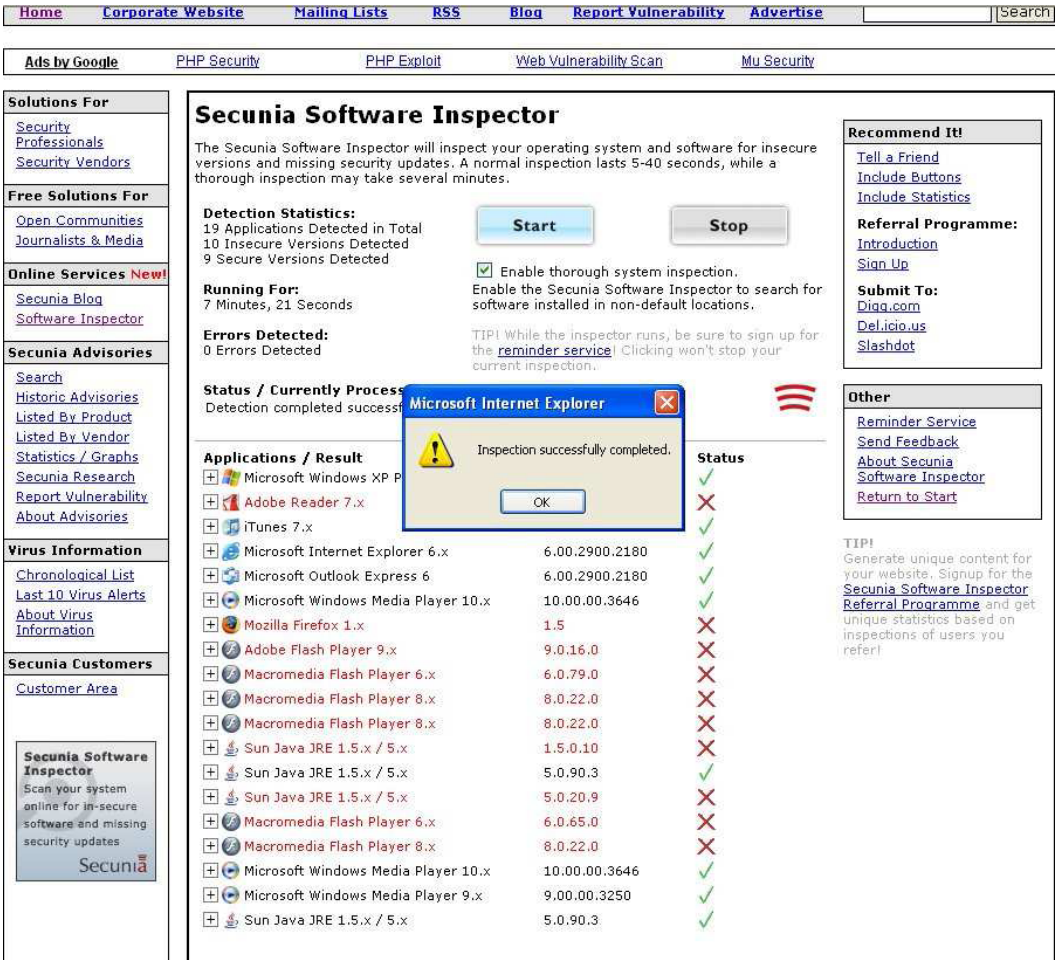
L'ORDINATEUR BIEN PROTÉGÉ ET SÉCURITÉ APPLIQUÉE

Primordial et obligatoire est aussi le téléchargement des mises à jour des logiciels dits indispensables (Macromedia Flash®, Adobe Acrobat Reader®, Java®, QuickTime®, ITunes®, VLC Media Player, Open Office, Firefox, Internet Explorer, etc.).
Ces applications représentent parfois des vulnérabilités critiques, voir même hautement critiques qui permettraient à un malfaiteur de prendre le contrôle de l'ordinateur à votre insu.

Secunia propose deux versions, une version de contrôle gratuite en ligne et une version plus complète comme téléchargement.

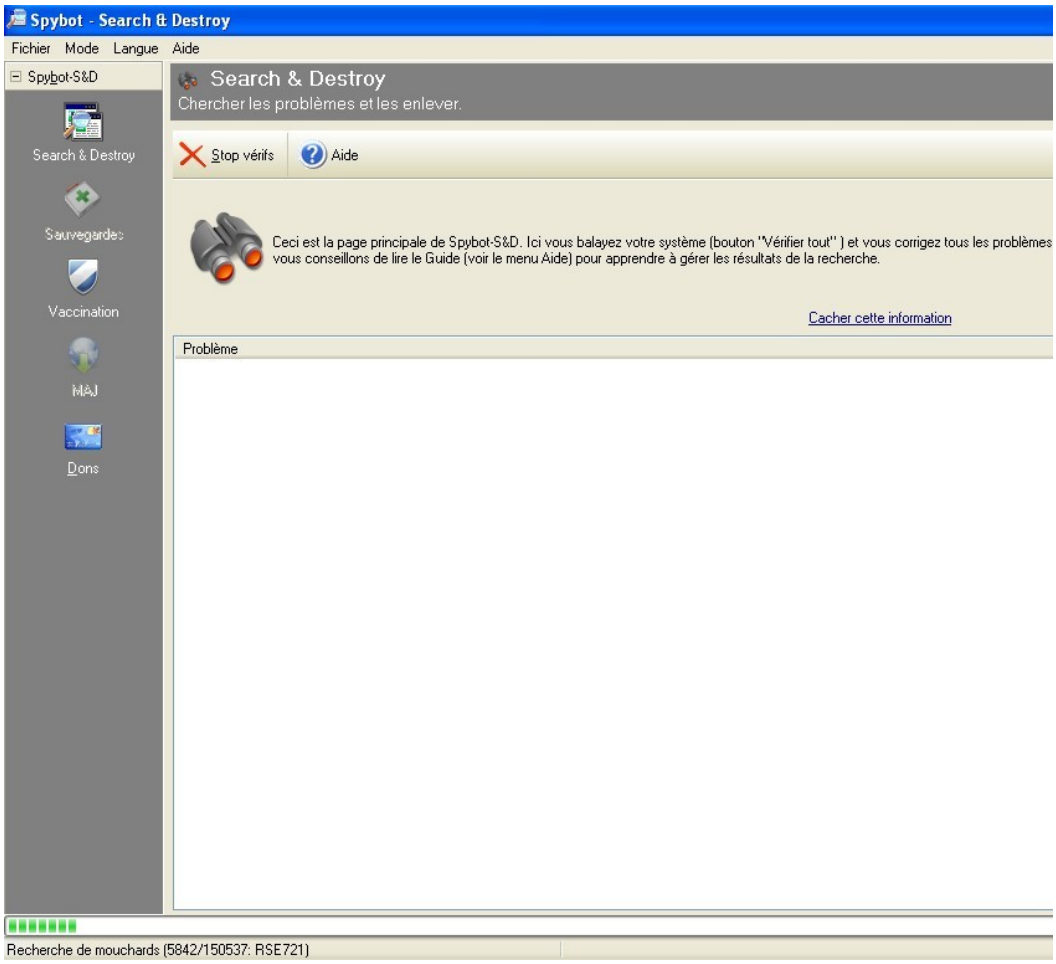
Un didacticiel, qui vous guide à travers l'utilisation, peut être téléchargé à l'adresse URL :

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



Les antispywares (anti mouchards)

Spybot Search&Destroy, logiciel « anti mouchard » gratuit et performant.



Visitez le didacticiel à l'adresse URL :

http://www.internetmonitor.lu/download/Spybot_S_D_Tutorial.pdf qui vous guidera à travers l'installation et l'utilisation.

Paul et Marie INNOCENT-INSOUCIANT

Les propriétaires

Georges LEMEILLEUR

Son créateur

Dominique PASMONPROBLEME

Son revendeur

Gérard J'YPEURIEN

Son réparateur

Ont le triste devoir de vous faire part du décès subit de leur ordinateur

Black Box Chéri

Né AB07/B785/-937/565-15B

Survenu à son domicile, le 08 novembre 2007, à l'âge de 3 mois.

Il n'avait malheureusement pas été sécurisé par ses propriétaires et fût attaqué par un botnet (autres ordinateurs non-sécurisés et infectés, et téléguidés par la mafia informatique) et il a succombé à ces infections !!!

Sa tour repose dans le bureau des INNOCENT-INSOUCIANT
123, Rue des Malinformés
L-1234 CAPOUT (Département du FOUTU)