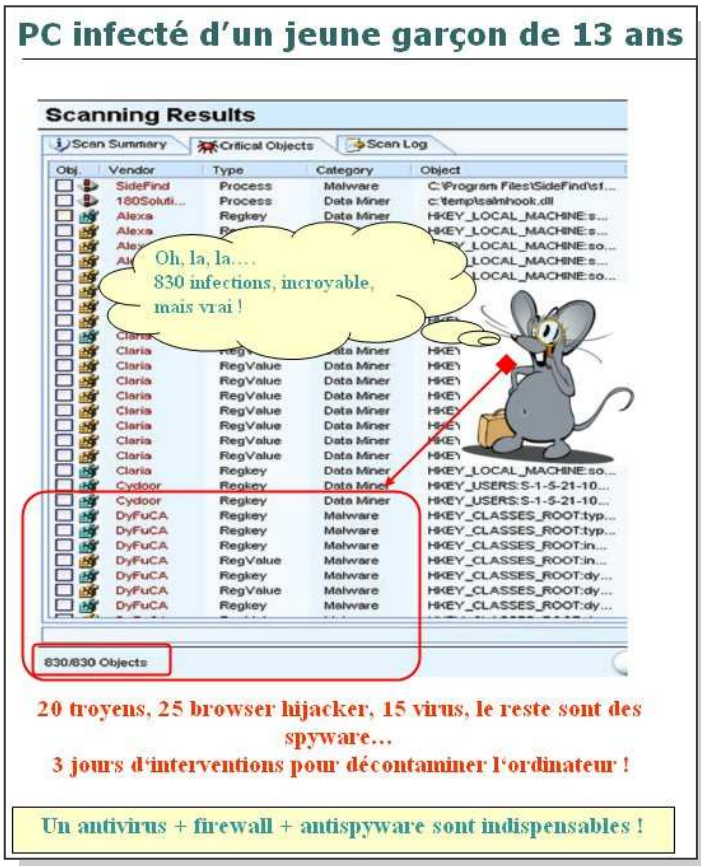
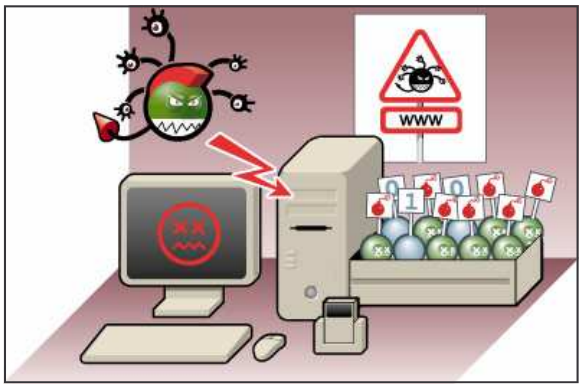
SECURITY MONITOR

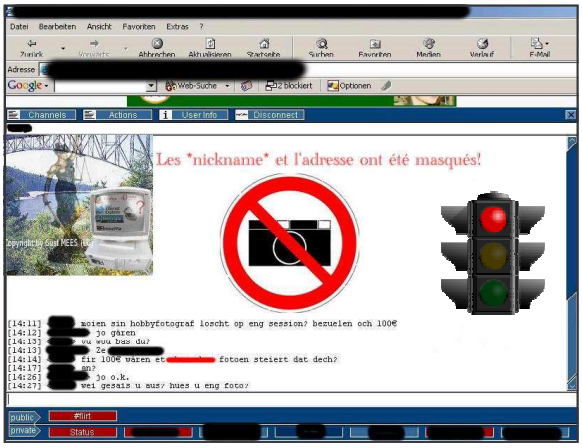
PC Sécurité

Octobre 2007

Mieux vaut prévoir que guérir !







Apprenez à vous protéger et à devenir vigilant avec des conseils simples à utiliser !

Édition spéciale :

- **Protection de l'ordinateur et contrôle de la sécurité.**
- **Les risques et la législation.**

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

SOUS WINDOWS® XP/LES CONSEILS DE MAUSI, LA SOURIS LUDIQUE !

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®, 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

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

L'ORDINATEUR BIEN PROTÉGÉ/LES CONSEILS DE MAUSI, LA SOURIS LUDIQUE !

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)** :

- **SuperAntispyware** : 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).

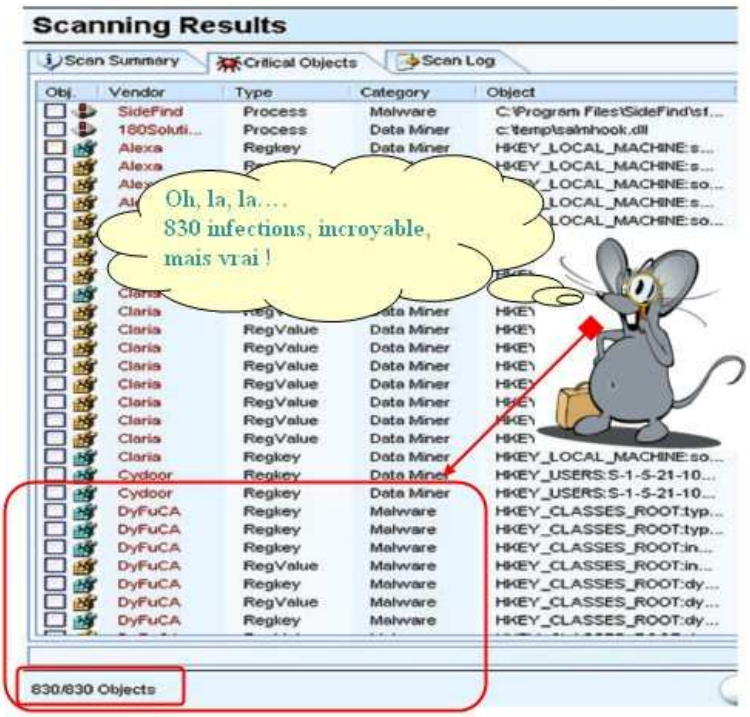
Par conséquent le conducteur d'un moyen de transport, **un être humain, n'est pas toujours attentif et court des risques ! L'être humain n'est pas parfait, loin de là !!!**

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

POURQUOI ÊTRE PROTÉGÉ ? LES CONSEILS DE MAUSI, LA SOURIS LUDIQUE !

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.

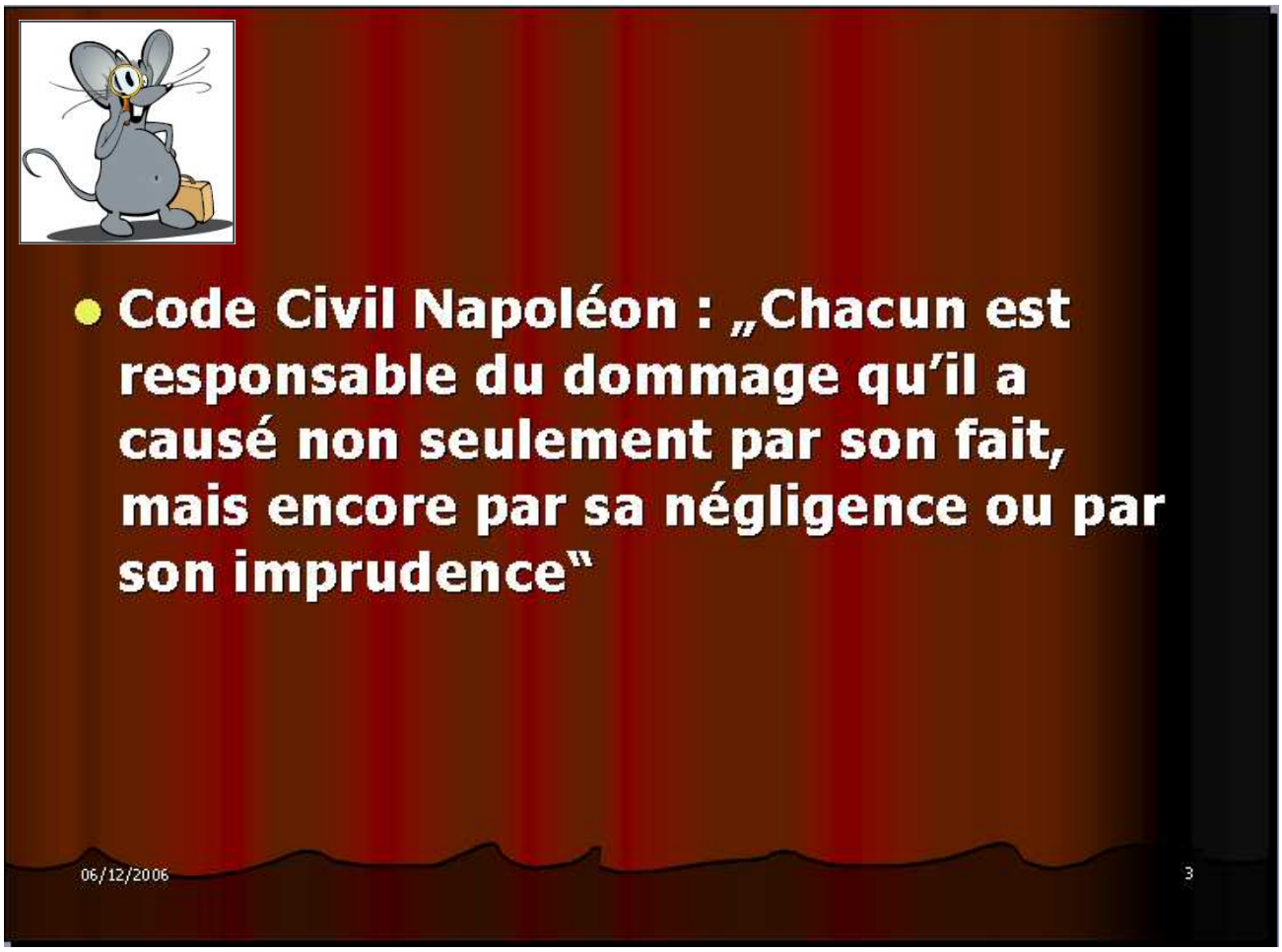
Un ordinateur infecté et qui est connecté à Internet distribue son (ses) infection (s) aux autres ordinateurs non sécurisées connectés à Internet !!!

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 !!!

CE QUE DIT LA LOI LUXEMBOURGEOISE !



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

Les lois chez nos voisins :

Droit du net (France) :

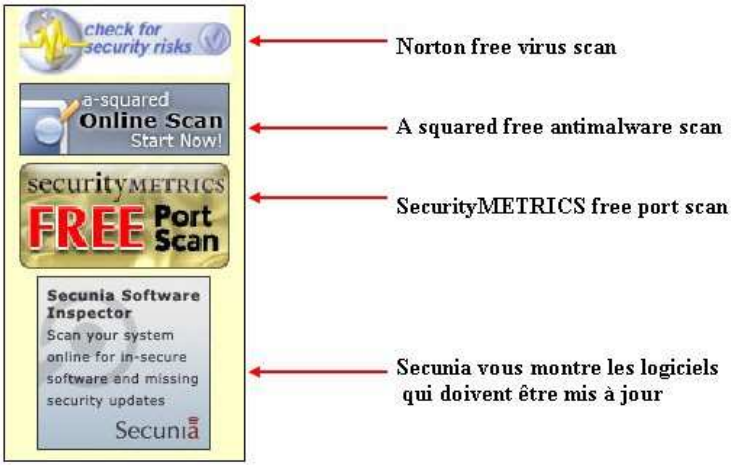
http://www.droitdunet.fr

Contrôle de la sécurité

L'ORDINATEUR BIEN PROTÉGÉ/LES CONSEILS DE MAUSI, LA SOURIS LUDIQUE !

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 toolbar

„**L'Internet Monitor**" vous propose aussi le téléchargement et l'utilisation gratuite de sa **barre d'outils** (**toolbar**) 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/LES CONSEILS DE MAUSI, LA SOURIS LUDIQUE !

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 „**MacAfee 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.myschool.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.

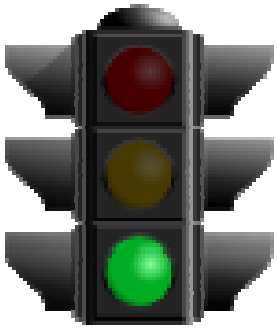
Conseils de sécurité et savoir-faire

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 que vous ne connaissez pas encore, veuillez utiliser „Wikipedia", dont voici le lien :

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 !!!

Conseils de sécurité, savoir-faire et information

L'ORDINATEUR BIEN PROTÉGÉ ET SÉCURITÉ APPLIQUÉE

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 national « 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 !!!