SURFEZ SUR INTERNET EN TOUTE SÉCURITÉ

Déjouez les pièges d'Internet

Tout ce que vous devez savoir pour :

Protéger vos enfants
Sécuriser votre ordinateur
Eliminer virus et spams

Guide offert par

Services-PC
www.services-pc.net

Table des matières

Avant-propos

Pourquoi ce guide ?

L'objectif de ce guide est de répondre aux nombreuses questions récurrentes que se posent les internautes lorsqu'ils surfent sur Internet. En effet rares sont les personnes pleinement conscientes des risques inhérent à l'utilisation d'Internet. D'autres personnes en ont une vision limité et erronée et vont jusqu'à se priver de cet outil qui est aujourd'hui incontournable dans la vie de tous les jours.
Ceux d'entres vous qui se posent encore la question s'ils doivent ou non « s'y mettre », que vous soyez jeune ou vieux, n'avez pas encore mesuré l'ampleur des bénéfices que vous pouvez en tirer. Pour en revenir à ce guide, le but est de vous fournir les moyens pour profiter pleinement d'Internet et de vous permettre de déjouer les pièges liés au surf sur Internet pour vous, votre famille et vos amis.
Il a aussi un rôle de sensibilisation et il ne saurait être exhaustif étant donné le nombre de sujets abordés. Nous vous proposons des renvois vers des sites Internet que nous avons choisis pour vous pour la qualité de leur contenu et les explications claires et simples qu'ils donnent.
Son rôle est aussi de vous donner les explications qui vous permettront de comprendre et de mieux appréhender les mécanismes sous-jacents utilisés par l'Internet.
Les explications ont été volontairement simplifiées afin de faciliter la compréhension par le plus grand nombre. D'avance nous nous excusons auprès des experts informatiques. D'autre part il est impossible de détailler dans ce guide, voué à la sensibilisation, tous les aspects liés à la sécurité informatique sur Internet. En effet, Internet fait appel à tant de technologies différentes qui peuvent être autant d'opportunités pour les pirates pour arriver à leurs fins qu'il faudrait une encyclopédie pour en faire l'inventaire !
Le nombre de technologies utilisées va en augmentant, cela risque de devenir problématique si les concepteurs de ces technologies ne prennent pas en compte en amont la sécurité. Internet est aujourd'hui une technologie mature, votre ordinateur est un moyen d'accès à Internet alors prenez soin de lui.
Mieux vaut prévenir que guérir...

Internet : à quoi cela va bien me servir ?

Internet vient de la contraction des mots « Inter » et « network » un mot anglais qui signifie interconnecter des réseaux informatiques entre eux. Pour faire simple à l'origine, Internet, dans les années 50/60 permettait de relier des ordinateurs d'un centre de recherche entre eux puis d'interconnecter plusieurs centres de recherches scientifiques, militaires et universitaires aux Etats-Unis.
Pourquoi cette volonté de relier des réseaux d'ordinateurs entre eux ? D'une part pour faciliter les communications et d'autre part pour le partage de l'information et du savoir. Là est la puissance d'internet ! Permettre à des milliards d'individus à travers le monde d'accéder à un savoir encyclopédique en utilisant un simple ordinateur !
Bien sûr au fur et à mesure le nombre d'ordinateurs interconnectés et leurs contenus, n'a cessé de croitre et continuera de croître encore exponentiellement. Votre ordinateur relié à internet fait partie intégrante de ce réseau mondial. On parle d'internet comme d'un monde virtuel mais c'est bien de millions d'ordinateurs bien réels, reliés entre eux qu'il s'agit. C'est l'information qui circule dans ce réseau qui n'est pas palpable donc virtuelle. Dès qu'elle s'affiche sur votre écran là elle n'est plus virtuelle ! Car vous pouvez à ce moment là l'imprimer, l'enregistrer ou « l'emprisonner » en la gravant sur un CD-ROM.
Tous les ordinateurs présents sur ce réseau ne jouent pas le même rôle. Votre ordinateur est relié au réseau mondial par le réseau de votre fournisseur d'accès à Internet (FAI pour les intimes) qui est lui-même relié à d'autres réseaux dans le monde. Pour simplifier, l'information, les sites internet, sont « hébergés » par des ordinateurs spécifiques appelés serveurs. Serveurs parce que tout simplement leur rôle est de « servir », de « donner » l'information et leur contenu à l'internaute qui le demande.

Un site Internet est un moyen par lequel l'information est présentée et organisée pour être consultée par l'internaute. Il existe des millions de sites internet qui traitent de tous les sujets imaginable et inimaginable !
Vous êtes passionné par la littérature anglaise du 18ème siècle ? Il est sûr et même certain que vous trouverez un site internet ou un blog traitant de ce sujet.
Liste non exhaustive de ce que vous pouvez faire sur Internet :
Acheter n'importe quoi (enfin presque !)
Comparer les prix des cybermarchands en un clic de souris
Vendre vos objets
Partager votre savoir ou vos connaissances en créant un blog ou un site Internet
Aider les autres internautes en donnant de votre temps sur les forums par exemple
Communiquer avec votre voisin ou avec le reste du monde
Faire des démarches administratives à distance
Comparer les prix des carburants des stations de service proche de chez vous
Planifier votre itinéraire (train, voiture, avion, bateau, vaisseau spatial avec VirginGalactic.com)
Connaître l'état de la circulation automobile, des transports en communs etc…
Consulter la météo, votre horoscope ou le programme TV de la semaine…
Ecouter les radios du monde entier

Internet à l'image du monde réel

Comme indiqué précédemment, Internet est loin d'être un monde virtuel car souvenez vous qu'il y a toujours un être humain derrière un ordinateur (photo de la page de couverture). Gardez toujours cela à l'esprit quand vous surfez sur Internet. Pour cette raison, Internet reprend les travers et les excès de l'être humain. Il faut donc être extrêmement vigilent lorsque vous ou vos enfants surfez sur Internet. Vous pouvez arriver au détour d'une page Internet sur des photos ou vidéos choquantes, des escrocs de tous poils, de faux sites Internet etc…

Il arrive que des associations douteuses se créent entre des sites Internet pornographique ou des sites de jeux en ligne et des pirates informatiques pour infecter un maximum d'ordinateur des internautes ayant visité ces sites volontairement infectés ! Le pirate rémunère ensuite les sites Internet en fonction du nombre d'ordinateurs infectés. Il se constitue ainsi un réseau d'ordinateurs qu'il peut manipuler et monnayer au plus offrant. Vous allez voir plus loin que les pirates informatiques ne manquent pas d'idées pour arriver à leurs fins.

Evitez les pièges d'Internet

Chapitre 1

Dans ce chapitre vous trouverez une liste non exhaustive des principaux vecteurs de propagation de programmes malicieux qui peuvent rendre votre ordinateur inutilisable. En effet, différents moyens sont utilisés par les pirates informatiques pour propager les infections informatiques. Vous vous demandez peut être pourquoi faut il prendre des précautions pour surfer sur Internet ? Pourquoi existe-t-il tant de menaces sur Internet et dans quel but ?

Il existe aujourd'hui des individus ou des bandes organisées en mafia pour tirer profit de votre ignorance des risques encourus sur Internet. L'objectif numéro 1 de ces individus qui propagent virus et mouchards informatiques est de prendre le contrôle de votre ordinateur grâce à ces programmes malicieux.

La prise de contrôle de votre ordinateur est le stade ultime de l'infection de votre ordinateur. Les pirates informatiques en profitent ensuite pour monnayer au plus offrant l'accès ou l'utilisation de votre ordinateur et de votre connexion à Internet. Hé oui, votre ordinateur et votre connexion Internet se revendent au plus offrant ! Des pages internet publicitaires s'ouvrent sans que vous n'ayez rien demandé ? Vous accumulez les barres d'outils dans votre navigateur web ? Il ne faut pas chercher bien loin pour deviner que votre ordinateur est infecté par un ou plusieurs adware ou spyware !
Les pirates jouent aux gendarmes et aux voleurs avec les concepteurs de logiciels antivirus pour être toujours en avance sur ces derniers. Votre ordinateur et plus exactement ce que l'on nomme le système d'exploitation n'est pas fiable à 100%.

Il existe donc des failles dans le système par lesquelles les programmes malveillants s'installent à votre insu dans votre ordinateur simplement en ayant visité un site Internet ou en ayant été trop confiant en téléchargeant et en installant un logiciel gratuit ou un logiciel payant piraté sur Internet. Vous comprenez aisément que le principal vecteur d'infection de votre ordinateur c'est vous ! Utilisateur lambda n'ayant pas connaissance des différentes menaces informatiques. Plus après avoir lu ce guide bien sûr !

Cybercriminalité : les tarifs de revente

Prestation	Tarif
Informations de cartes de crédit, prix en fonction des données recueillies : code, date d'expiration, nom du propriétaire…	2 à 25 $
Compte PayPal	7 $
Compte World Of Warcraft (jeu en réseau sur Internet)	8 $
Infection de 1 000 systèmes	15 $
1 million d'adresses e-mail	25 à 50 $
Par attaque de déni de service avec les 10 premières minutes offertes, puis 20 $ l'heure et 100 $ la journée	25 à 100 $
20 millions de spams pendant 14 jours	495 $
Par exploit (programme exploitant une faille de sécurité)	100 à 3 000 $
La faille de sécurité inconnue	5 000 à 50 000 $

(Source : laboratoire de sécurité G Data 2007-2008) ODI numéro 49

Les logiciels gratuits

Vous trouverez énormément de programmes plus intéressant les uns que les autres et dits gratuits. La plupart du temps les concepteurs de ces programmes ne demandent pas de contrepartie à l'utilisation de leurs logiciels. Il arrive que souvent ils demandent simplement un don en argent à la discrétion de l'internaute pour soutenir le développement de leur logiciel. D'autres personnes ou entreprises indiquent qu'en contrepartie de l'utilisation de leurs logiciels, des informations concernant vos habitudes de surf seront envoyés vers Internet ou des fenêtres publicitaires risquent d'apparaître de manière aléatoire. Rien n'est jamais gratuit sur Internet il existe toujours une contrepartie à l'utilisation d'un programme gratuit.

Les faux Codec et les ActiveX

Un codec est un outil logiciel qui permet de décoder ou coder un document audio ou vidéo. Certains sites pornographiques ou humoristiques vous demandent de télécharger et d'installer un codec pour que votre logiciel de visionnage de vidéo puisse lire ces vidéos. Or ce n'est pas un codec que vous installerez mais bien un programme malveillant !
Un ActiveX est aussi un outil logiciel. Il sert à votre navigateur Internet Explorer pour afficher les pages web d'un site Internet complexe. Le problème c'est que certains sites Internet sont conçus de telle manière à installer à votre insu un programme malveillant une fois que vous l'avez visité. Vous verrez ensuite rapidement les premiers « symptômes » apparaître :
• fausses alertes de sécurité,
• modification du fond d'écran,
• détournement de la page d'accueil de votre navigateur internet
• installation non désirée de faux logiciels de sécurité proposant leurs services payants pour nettoyer l'infection.

Le chantage

Les pirates ne manquent pas d'imagination pour vous soutirer de l'argent ! Une fois votre ordinateur infecté par leur programme malicieux, celui-ci va crypter vos fichiers et les rendre inutilisables tant que vous n'aurez pas payé une rançon pour les décrypter !

Les faux logiciels de sécurité

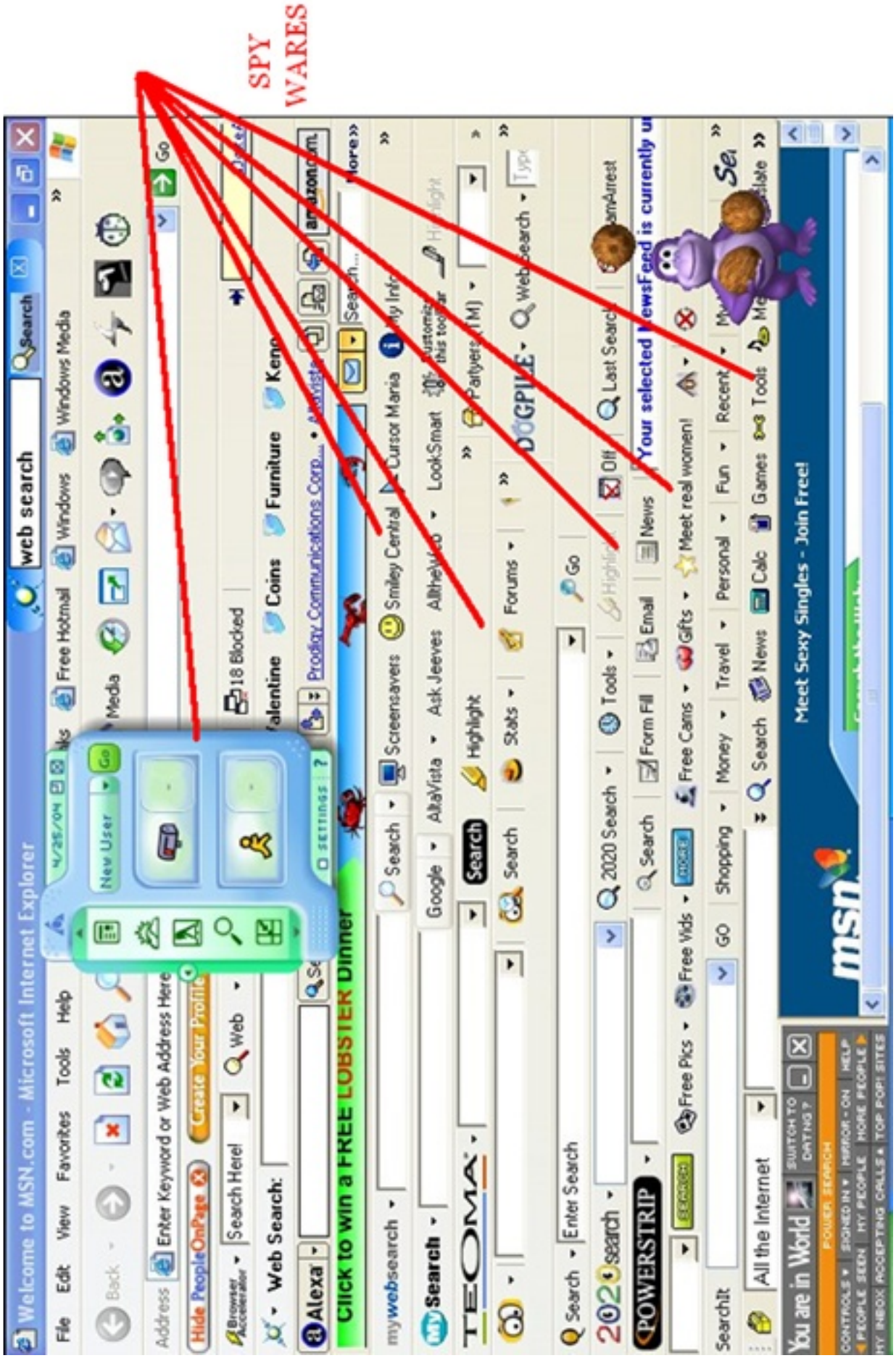
Comme indiqué ci-dessus ce genre de logiciel ne s'installe qu'avec votre accord ou à votre insu si votre ordinateur n'est pas à jour. En effet, certains sites internet volontairement mal conçus exploitent les failles de votre ordinateur non tenu à jour.
Il en existe plusieurs catégories: anti spyware, antivirus... Le but de ces faux logiciels est de pousser l'utilisateur à acheter une licence payante:
Soit via des publicités sur des sites WEB qui redirigent vers les sites qui conçoivent ces faux logiciels.
Soit en installant des infections sur votre ordinateur:
• affichage de bulles d'alertes disant que votre ordinateur est infecté.
• modification de votre fond d'écran en disant que votre ordinateur est infecté.
• modification de la page de démarrage de votre ordinateur vers des sites affichant de fausses alertes de sécurité
A noter que les alertes sont en général en langue anglaise. Chaque alerte propose de télécharger ce type de logiciel. Une fois le scan (totalement mensonger) de l'ordinateur effectué par le programme, ce dernier affiche qu'il faut acheter la version commerciale pour nettoyer l'ordinateur. Le but est donc de faire peur et de forcer la main, via des alertes incessantes, à acheter ces logiciels totalement inutiles. En page suivante WinAntivirusPro 2007 est un faux logiciel Antivirus !

Pirater les logiciels payants

Beaucoup d'internautes s'adonnent au téléchargement de programmes payants. Ils essaient ensuite d'enlever les protections à l'aide d'un programme appelé communément crack ou inscrivent un numéro de série généré par un keygen. Toutes ces applications facilitant le piratage ne sont pas forcément contaminées, mais les auteurs de malwares piègent ce type de programme pour faciliter la diffusion de leurs programmes malicieux. Ainsi, en pensant faire sauter la protection d'un logiciel, l'utilisateur trop confiant exécute un programme malveillant avec ses droits d'administrateur, ce qui permettra l'infection du système.

Sachez que les auteurs de malwares créent de faux sites Internet de cracks où tous les cracks proposés sont infectieux, d'autres sites eux contiennent des exploits, si votre navigateur n'est pas à jour, c'est l'infection assurée.

En outre, certaines infections issues de cracks proposés sur les réseaux P2P, une fois installées mettent à disposition des cracks piégés sur le réseau P2P pour que d'autres internautes les téléchargent et s'infectent à leur tour !


SPY
WARES
Welcome to MSN.com - Microsoft Internet Explorer
web search
Click to win a FREE LOBSTER Dinner
Meet Sexy Singles - Join Free!
msn

Les canulards et le hamçonnage (Phishing)

Nous sommes tous confrontés à des Hoax: Ce sont des canulars qui circulent sur Internet et qui sont véhiculés par mails. Vos proches souhaitent vous faire partager une information qu'ils jugent importante alors qu'en fait, ce n'est qu'un leurre destiné à engorger le réseau Internet. Ce sont le plus souvent de fausses alertes de virus ou, ce qui est bien plus pervers, de fausses chaînes de solidarité.
Tout mail se terminant par des phrases du type « envoyez ce mail à tous vos contacts pour ... » demandant à propager l'information est certainement un hoax, vérifiez la véracité du contenu du mail.
Depuis quelques années, les pirates du web s'attaquent à une nouvelle forme d'escroquerie en masse via le phishing: Ils spamment des milliers d'internautes avec des messages dans le but de leur voler des informations bancaires. Leur procédé est très astucieux: ils envoient un mail avec un lien vers un site qui ressemble "presque" parfaitement au portail de votre banque. "Presque" car l'adresse n'est pas la même et jamais une banque ne vous demanderait des informations confidentielles en ligne.


LCL
LE CRÉDIT LYONNAIS

Cher client de **LE CRÉDIT LYONNAIS,**

Le département technique de LE CRÉDIT LYONNAIS procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.

http://www.lcl.fr/banque/secure/portail/confprocedure.asp

Nous nous excusons pour tout désagrément et vous remercions de votre coopération.

©LE CRÉDIT LYONNAIS 2006

<

http://www.lcl.fr.banque.secure.mgmcomps.com/r1/cl/>

L'internaute trop confiant enverra ainsi des informations bancaires à ces pirates et le résultat ne se fera pas attendre: les pirates n'ont plus qu'à se servir de ces informations pour ponctionner de l'argent sur son compte en banque. Il est vrai que depuis les banques verrouillent le module de virement européen ou international avec une sécurité supplémentaire qui empêche le pirate de transférer de l'argent.
La règle est donc simple: Ne jamais fournir d'informations confidentielles même si c'est votre banque qui en fait la demande. Les organismes bancaires connaissent suffisamment ces questions de sécurité pour ne pas faire ce genre de choses. De plus tous les secteurs sont touchés, pas seulement les banques, c'est pourquoi ne il est recommandé de ne pas ouvrir ce type de message et de na pas cliquer sur les liens inclus dans ces messages.

SOCIETE GENERALE: LE MESSAGE URGENT [Tue, 21 Mar 2006 03:48:56 -0800]

Fichier Edition Affichage Outils Message ?

Répondre Répondre ... Transférer Imprimer Supprimer Précédent Suivant Adresses

De : ©Societe Generale
Date : lundi 20 mars 2006 20:39
À :
Objet : SOCIETE GENERALE: LE MESSAGE URGENT [Tue, 21 Mar 2006 03:48:56 -0800]

SOCIETE GENERALE

Cher client de **SOCIÉTÉ GÉNÉRALE**

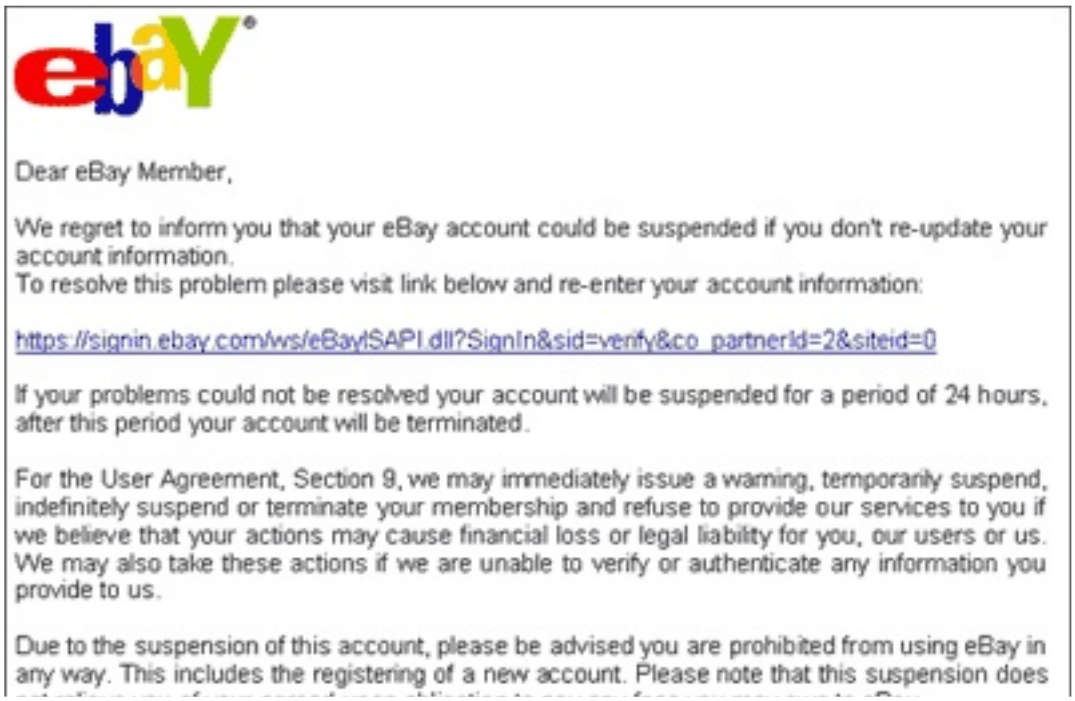
Le département technique de Société Générale procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.

http://www.societegenerale.fr/customercare/banque/confprocedure.asp

Nous nous excusons pour tout désagrément et vous remercions de votre coopération.

© Société Générale 2000-2006



ebay

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does

Les enregistreurs de frappe au clavier

On les nomme Keylogger. C'est un programme informatique malicieux installé sur votre ordinateur à votre insu via un email infecté ou utilisant un autre vecteur de propagation. Il permet d'enregistrer les frappes de touches du clavier et de les enregistrer, à votre insu. Le type d'information enregistré est assez variable : sites web visités, les courriers électroniques, les mots de passe, les numéros de carte bancaire etc…
En fait c'est un logiciel d'espionnage qui enregistre absolument tout ce que vous frappez au clavier. Les informations collectées sont ensuite envoyées vers un serveur sur Internet ! Le pirate n'a plus ensuite qu'a rechercher les informations utiles parmis cet amas de données. Inutile de vous préciser le type d'information qu'il recherche... Le pire, c'est que ces informations vont pouvoir lui servir pour mieux affiner et préparer ses futures attaques via le phishing ou tout autre méthode sur sa cible. Cela afin de mieux berner sa victime !

Les sites Internet à éviter

Les failles de sécurités permettent d'infecter votre ordinateur automatiquement et à votre insu.
A l'heure actuelle les failles sur les navigateurs WEB sont très exploitées, ces failles permettent via la consultation d'un site internet malicieux d'infecter votre ordinateur de manière automatique. Le seul rempart, si votre navigateur internet est vulnérable, reste votre antivirus, ces infections sont très souvent mises à jour afin de s'assurer que les antivirus ne puissent pas suivre la cadence. Les chances d'infections si votre navigateur WEB est vulnérable restent très élevées.
Les sites Internet à éviter : les sites pornographiques, les sites de logiciels pirates,
Potentiellement, n'importe quel site peut avoir été falsifié ou modifié sans que le propriétaire ou le concepteur du site ne soit au courant. En effet, certains hébergeurs de site ne protègent pas suffisamment l'accès à ces sites ou le propriétaire du site lui-même néglige l'utilisation de mot de passe fort.

Le détournement de votre ordinateur

Le détournement de votre ordinateur consiste à installer des programmes malveillants pour prendre le contrôle de votre ordinateur et l'utiliser à votre insu. Votre ordinateur infecté est appelé alors zombie car il est totalement contrôlé par un pirate sur Internet. Un ensemble de PC zombies infectés est appelé Botnet. Le pirate se prend alors pour Dieu car il peut, avec des centaines voir des milliers d'ordinateurs, monnayer « l'utilisation » de son réseau ! La plupart du temps, il envoie des spams (email non sollicités) à la terre entière en utilisant votre ordinateur et votre connexion Internet !
Pour arriver à leur fin, la plupart des infections se doivent de rester discrètes afin de rester le plus longtemps chez leurs hôtes. On pourra suspecter une infection dans le cas d'affichage de popups, ou par une activité douteuse du système, voire d'une connexion Internet très lente.

Les emails et la messagerie instantanée "tchat"

La messagerie instantanée est très utilisée pour discuter en direct par ordinateur interposés avec ses amis ou des inconnus sur Internet. Le problème c'est que la technologie utilisée, principalement Messenger ou Windows Live Messenger n'est pas très sécurisée. Il arrive souvent que des personnes se fassent infecter par ce biais.
Les emails sont le vecteur le plus utilisé pour vous induire en erreur et infecter votre ordinateur en profitant de votre incrédulité. Les personnes trop curieuses ont toutes tendances à ouvrir les messages contenant des mots très attractifs du type « sex », « Estelle veut te parler » ou des messages concernant l'actualité des « people » types « Britney Spears » ou autre.
Comme beaucoup de gens, vous recevez peut être plusieurs emails dont vous ne connaissez pas le destinataire qui vous incite à cliquer sur un lien ou à ouvrir une pièce jointe. La règle est plutôt simple : si vous ne connaissez pas le destinataire, supprimez le message. Même si le message paraît venir de Microsoft ou de votre meilleur ami, vous devez faire attention, car l'adresse de l'expéditeur peut très bien avoir été falsifiée ou votre meilleur ami peut être très bien infecté sans le savoir.
Ce qui est bien, c'est que la plupart des internautes ont compris qu'il ne fallait pas ouvrir des pièces jointes venant d'un inconnu.
Malheureusement, la méthode d'infection a évolué et il n'est pas rare de voir des vers par messagerie instantanée (comme MSN). Ces vers utilisent une méthode plutôt ingénieuse en se propageant par le biais de vos propres contacts et en vous incitant à cliquer sur un lien ou à ouvrir une pièce jointe. Le mieux est encore de ne pas cliquer bêtement, mais d'y réfléchir à deux fois et de se demander si le message est inoffensif ou pas.

Sites Internet utiles

https://informations.lcl.fr/securite/risques/index.html Site d'information sur la sécurité sur Internet de la banque LCL. C'est le complément idéal de ce guide

Sécurisez efficacement votre ordinateur

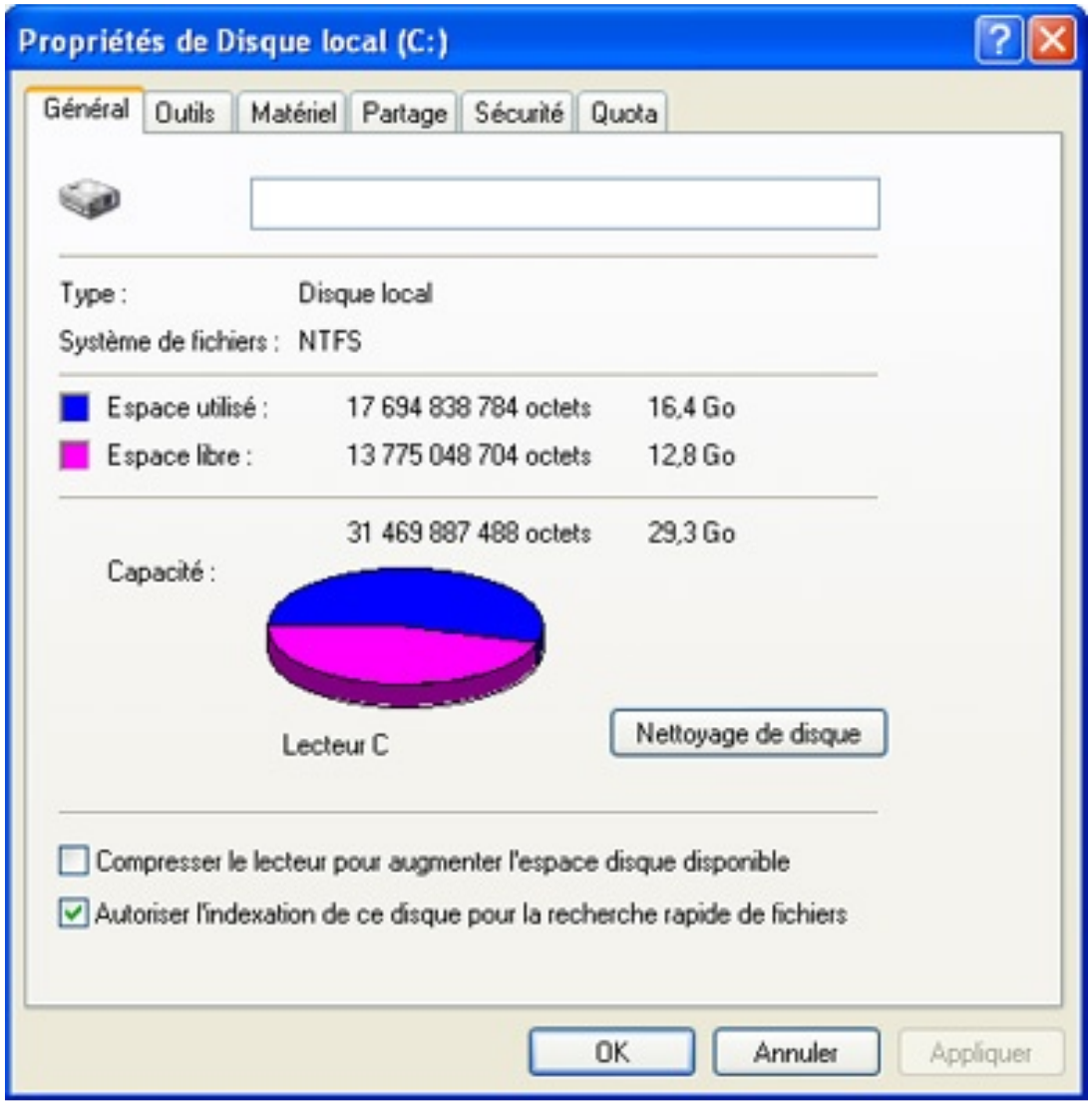
Chapitre 2

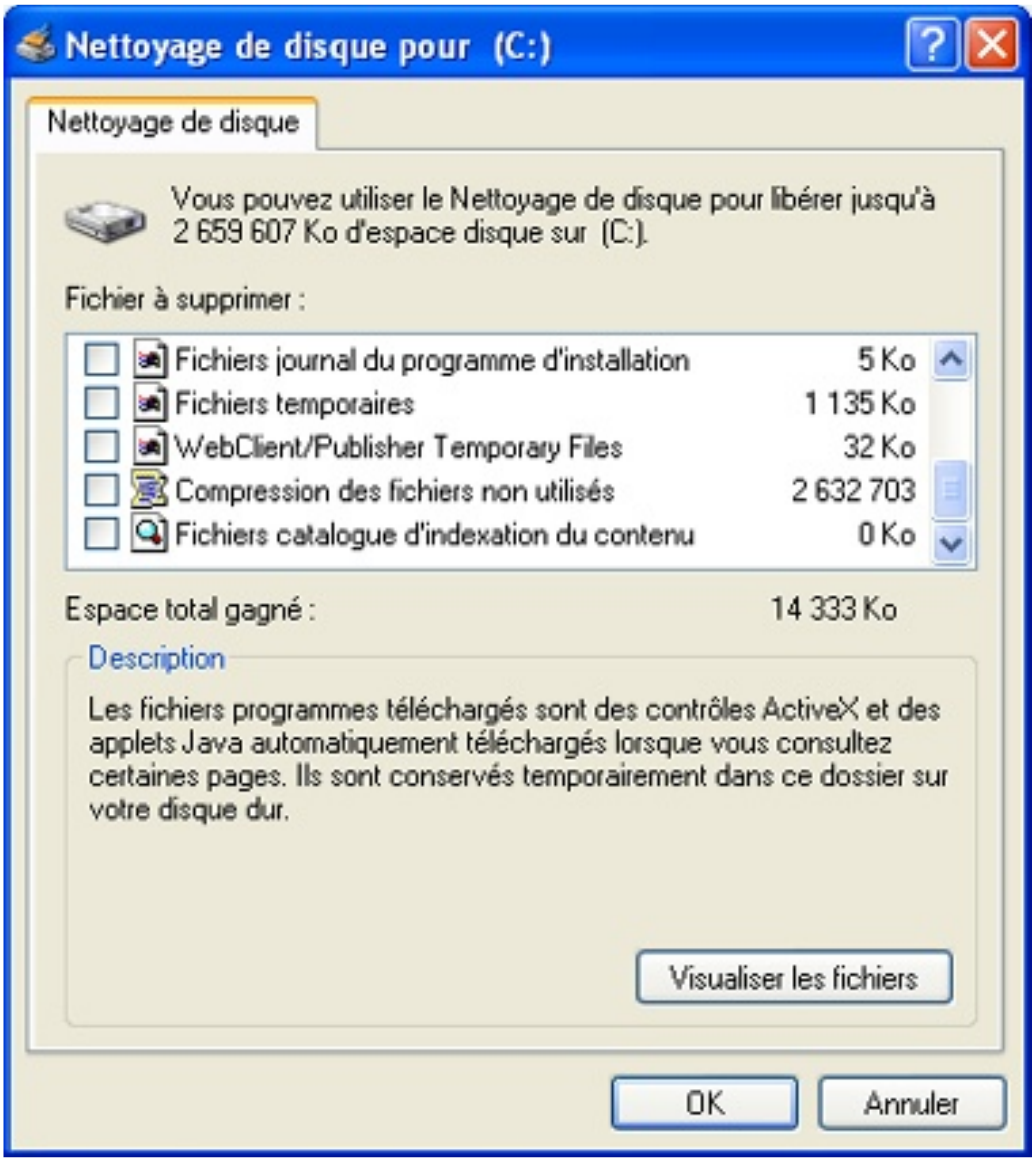
Vous commencez à comprendre, à ce stade du guide que le principal vecteur d'infection de votre ordinateur c'est vous ! Il vous faut donc faire preuve de vigilance, ne pas cliquer sur OK ou SUIVANT sans savoir ce que vous faites. Nous allons voir dans ce chapitre comment faire pour sécuriser votre ordinateur et éviter les dégâts si un programme malveillant venait à s'installer.

Faîtes un nettoyage régulier de votre PC

Votre ordinateur : le système d'exploitation et les programmes génèrent à chaque utilisation de nombreux fichiers dits temporaires qui deviennent inutiles et qui encombrent votre ordinateur. Plus vous surfez sur Internet plus ce type de nettoyage s'avère nécessaire cela pour éviter le ralentissement global de l'ordinateur. Plus le nombre de fichier est important, plus le risque d'infection sera élevé et plus le temps de recherche des programmes malicieux sera long pour l'antivirus.
Windows XP dispose d'un programme permettant de réaliser un nettoyage rapide. Pour lancer un nettoyage allez sur « DEMARRER » puis « POSTE DE TRAVAIL » puis faîtes un click avec le bouton droit de la souris sur le disque dur « C : » et sélectionnez « PROPRIETES »

Ensuite cliquez sur « NETTOYAGE DE DISQUE »



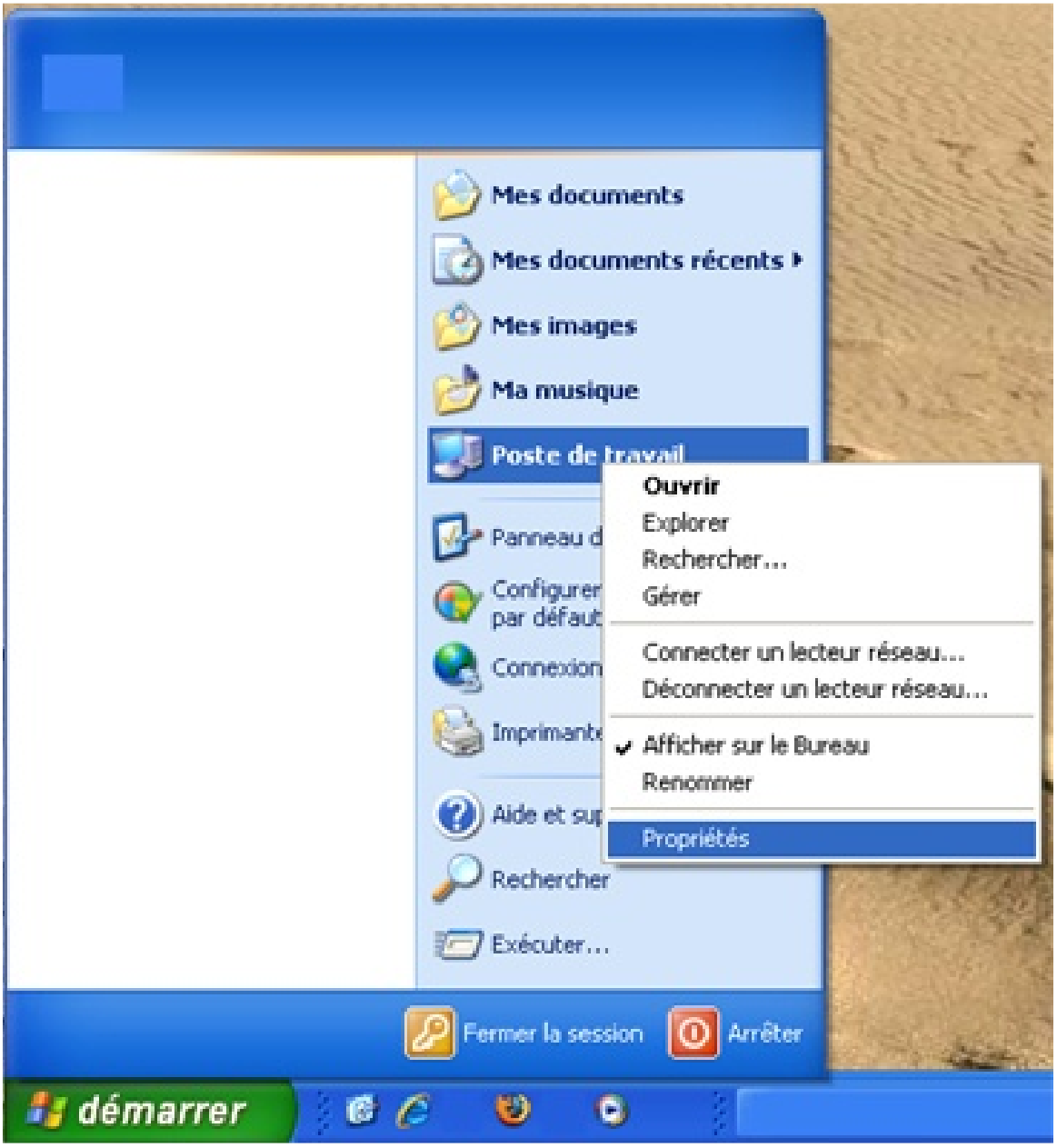


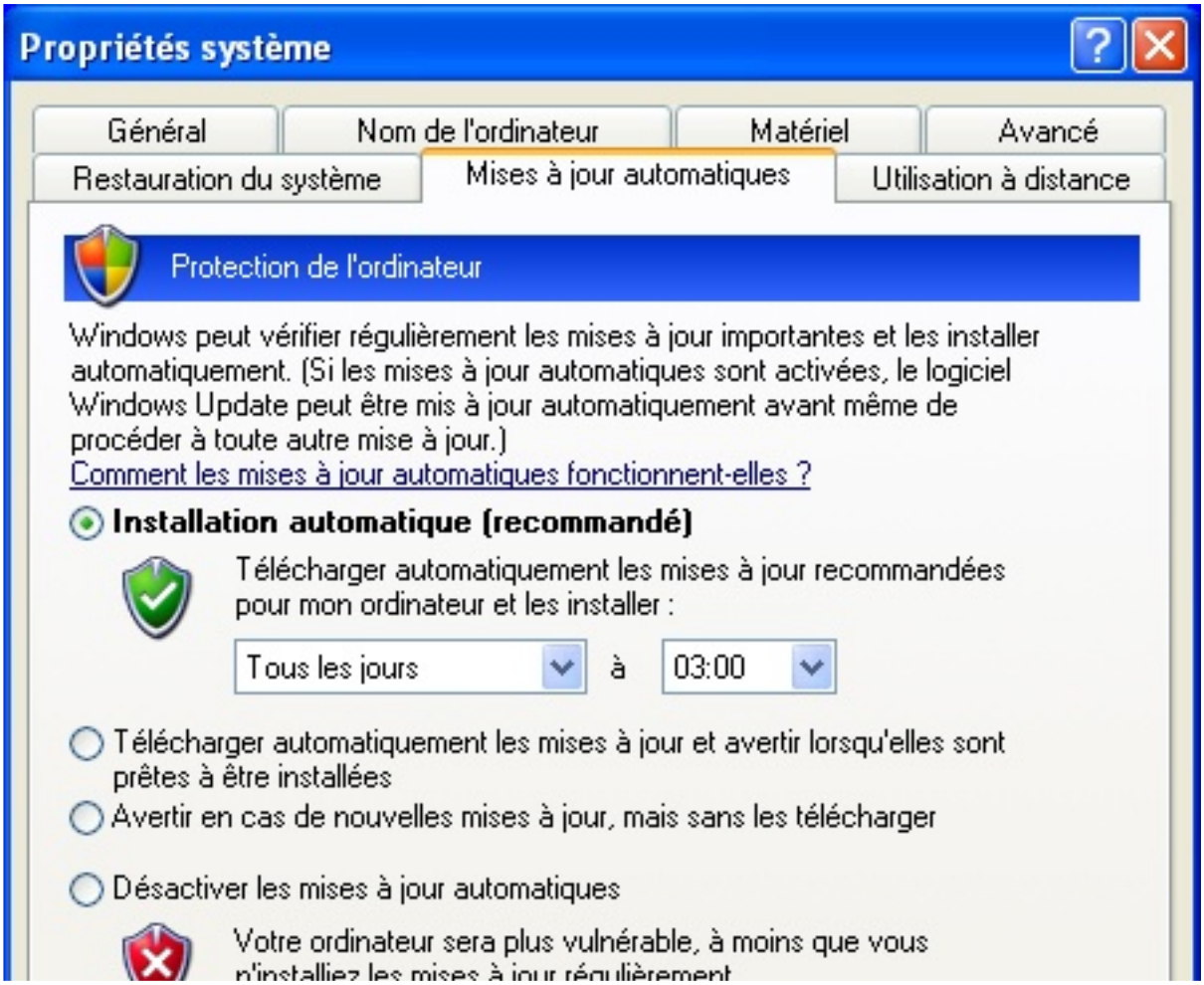
L'ordinateur recherche alors les fichiers inutiles et vous propose une liste avec l'espace que prend chacun des éléments trouvés. Dans l'exemple ci-dessus il vous suffit de cocher les éléments que vous souhaitez supprimer : « les fichiers internet temporaires » ou la « corbeille ». ATTENTION ne cochez surtout pas « Compression des fichiers non utilisés » !
Pour réaliser ce type d'opération plus simplement vous pouvez télécharger et installer un programme très simple qui permet d'un clic de souris de supprimer tous les fichiers temporaires de votre ordinateur. Il s'agit de CCLEANER que vous pouvez trouver sur le site Internet www.telecharger.com

Mettez votre ordinateur à jour

Votre ordinateur contient de nombreux programmes nécessaires à son bon fonctionnement dont un particulièrement important qui est appelé « Système d'exploitation ». Ces programmes ne sont pas exempts de défauts et ne sont pas fiables à 100%. De plus l'interaction du Système d'exploitation avec les autres programmes peut poser certains problèmes qui peuvent conduire à l'instabilité de

votre ordinateur.
Les mises à jour sont donc très importantes pour disposer des dernières versions des programmes présents sur votre ordinateur. Ces mises à jour permettent aussi de combler les fameuses failles de sécurités indiquées au début de ce guide. En effet, les pirates sont constamment à l'affut pour profiter de la moindre faille leur permettant d'introduire leur programme malveillant dans votre ordinateur à votre insu. Les mises à jour permettent aussi aux concepteurs des logiciels, de vous fournir de nouvelles fonctionnalités ou d'améliorer le fonctionnement de leurs programmes.
Pour mettre à jour Windows c'est à dire le système d'exploitation faîtes un click en appuyant sur le bouton droit sur "POSTE DE TRAVAIL" qui se trouve dans "DEMARRER". Voir la capture d'écran ci-dessous:

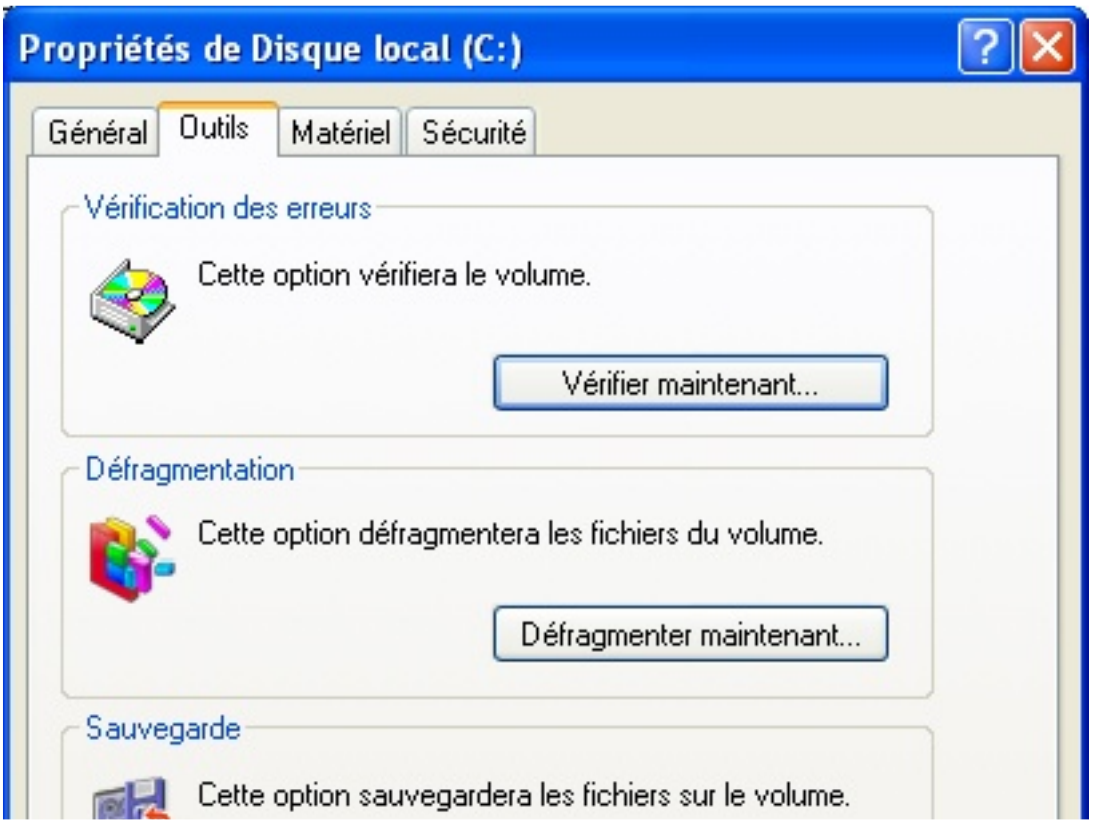




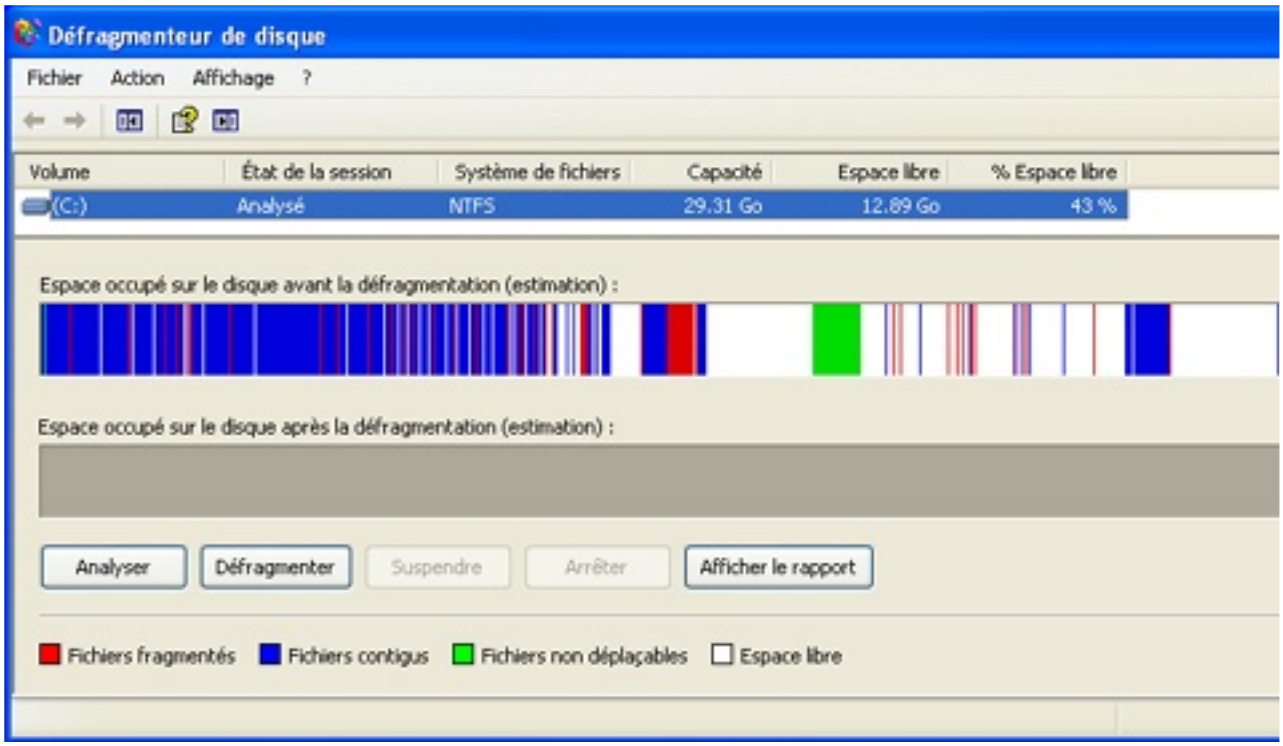
La fenêtre ci-dessus vous permet de régler la façon dont Windows doit se mettre à jour. Pour que les mises à jour se fassent automatiquement, cochez le premier choix "INSTALLATION AUTOMATIQUE" et choisissez la fréquence et l'heure de recherche de mises à jour. Indiquez une heure pendant laquelle l'ordinateur est susceptible d'être en fonctionnement. Validez ensuite votre choix en cliquant sur "OK".

Faîtes une défragmentation régulière

La défragmentation consiste comme son nom l'indique à regrouper les fragments de fichiers au même endroit sur le disque dur de l'ordinateur. Cela afin d'améliorer les performances globales de l'ordinateur. Il faut savoir que les fichiers ou documents de votre ordinateur peuvent être « découpés » en des milliers de fragments dispersés dans le disque dur. Dès que vous voulez accéder à ce fichier, il faut un certain temps au disque dur pour retrouver tous les fragments éparpillés. Imaginez que vous supprimiez un fichier, ce sont alors des milliers de fragments d'espaces vide qui vont se créer. Et ainsi de suite, à chaque création ou suppression de fichiers. Au bout d'un certain temps, le disque dur est tellement fragmenté que vous passerez plus de temps à « attendre » votre ordinateur qu'à travailler !

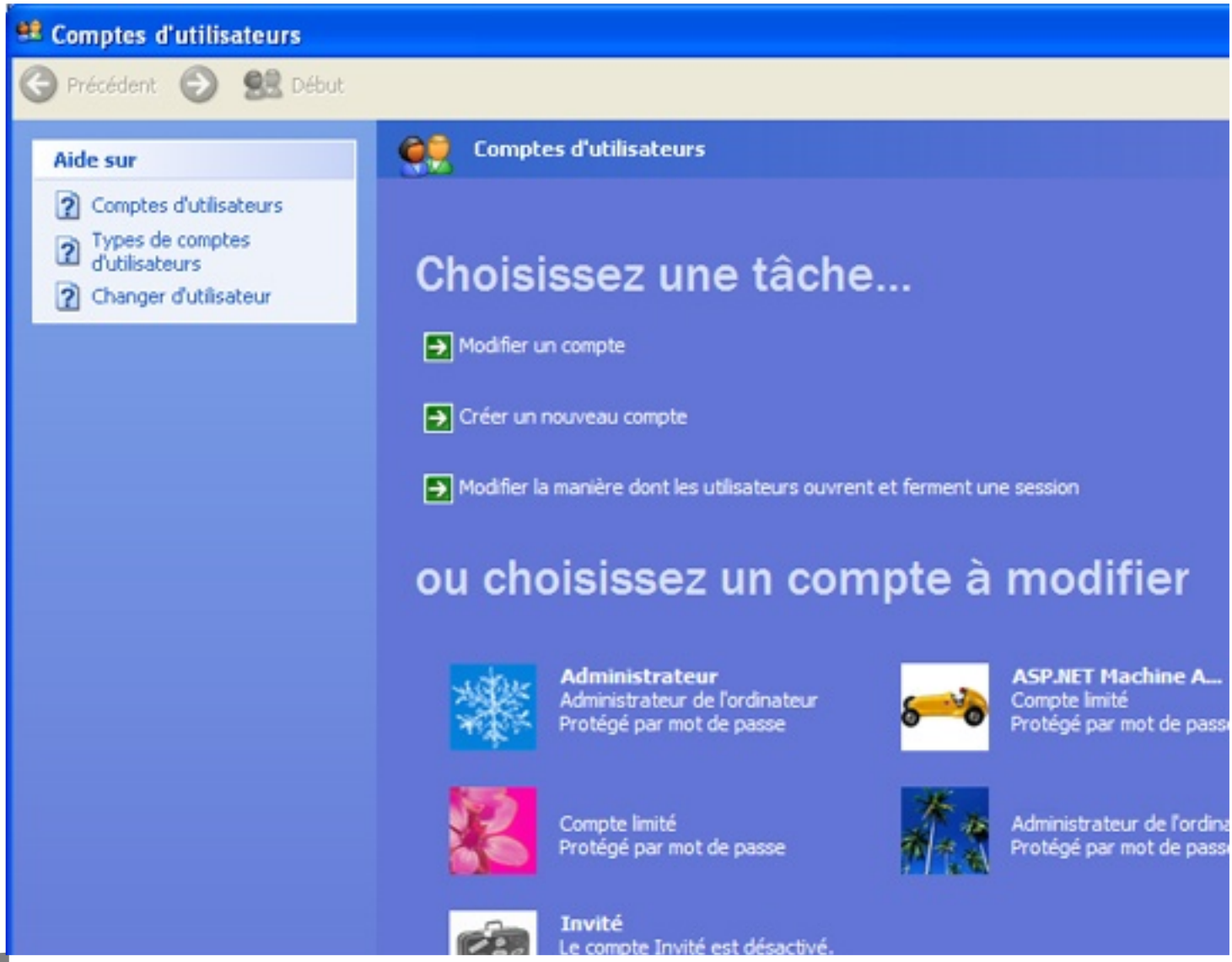


Pour afficher le défragmenteur de disque, procédez comme indiqué au début de ce chapitre pour nettoyer un disque dur sélectionnez l'onglet "OUTIL" et cliquez sur "DEFRAGMENTER MAINTENANT". Vous verrez apparaître la fenêtre ci-dessous. Il ne vous reste plus qu'a appuyer sur le bouton "DEFRAGMENTER" et laisser faire le programme jusqu'à ce qu'il vous indique qu'il a terminé.



Evitez d'utiliser le compte administrateur

Windows XP et Vista permettent de créer un ou plusieurs « compte d'utilisateur ». Imaginons que vous disposiez d'un ordinateur pour toute la famille, il est souhaitable de créer un « compte » pour chacun des utilisateurs de l'ordinateur. Cela permet d'une part d'empêcher un membre de la famille de supprimer par mégarde tous vos documents et d'autre part de cloisonner les documents de chacun des utilisateurs afin de les rendre « invisible » pour le reste des utilisateurs (confidentialité). Pour ce faire vous disposez de 2 comptes standards : le compte « administrateur » et le compte « utilisateur simple ou limité ». Le compte administrateur à accès à tous les endroits sensibles de l'ordinateur et y compris aux documents de tous les utilisateurs. Il permet d'effectuer toutes les opérations de maintenance et d'entretien de l'ordinateur. Il peut aussi installer n'importe quel logiciel. Le compte « utilisateur simple » permet à l'utilisateur d'utiliser les programmes déjà installés sur l'ordinateur, de surfer sur Internet, de créer ou supprimer ses propres documents enfin bref, d'utiliser normalement l'ordinateur. Il n'a pas accès à certaines zones protégées du système et il ne peut pas non plus installer de logiciel (certains programmes s'installent quand même).



Pourquoi ces précautions ?
L'objectif est simple : pour des raisons de sécurité, vous devez absolument éviter d'utiliser un compte administrateur pour l'utilisation courante de votre ordinateur (hors installation de logiciels ou d'opérations de maintenance). En effet, 99% du temps d'utilisation d'un ordinateur correspond à des tâches courantes : création de documents, surf, utilisation de logiciels, impression de documents etc…
Si vous utilisez un compte administrateur, le virus va usurper votre identité et se faire passer pour vous aux yeux du système d'exploitation et il va donc avoir accès, tout comme vous, à tous les endroits protégés de l'ordinateur. En effet, un virus est un programme informatique avant tout et il doit absolument s'enregistrer dans ces zones protégées pour pouvoir fonctionner. La seule différence avec l'installation d'un programme inoffensif, c'est qu'il ne vous affiche rien et ne vous demande pas votre avis !
Dans le cadre d'une utilisation familiale, il est recommandé d'utiliser pour chacun des membres de la famille, parents compris, un compte limité. Il suffit alors de garder le compte administrateur créé lors de la première mise en marche de l'ordinateur. Par contre il est particulièrement indiqué de protéger les comptes avec un mot de passe et vous vous en doutez, celui du compte administrateur avant tout !

Installez et paramétrez un antivirus complet

Selon un sondage réalisé par G Data auprès de 500 personnes, près de 47 % naviguent sans protection sur Internet ou disposent d'une protection dépassée ! L'antivirus ainsi que le pare-feu et l'antispyware sont les seules protections dont vous disposez pour vous éviter de laisser la porte ouverte aux virus. Si ce n'est pas déjà fait installez un antivirus gratuit ou payant.
Préferez au simple antivirus les solutions de protection complètes qui comprennent un antivirus, un pare-feu, un antispam, parfois un antispyware, un outil de surveillance de votre ordinateur et notamment de votre navigateur Internet, le scan à la volée des emails et pièces jointe, le téléchargement de fichiers sur la messagerie instantanée type MSN. La multitude des technologies employés par les pirates touche à toutes les parties de votre système d'exploitation et donc vous devez vous en prémunir avec ces solutions de sécurité complète.
De nouveaux virus ou des variantes de virus apparaissent chaque jour. Chaque nouveau virus est décortiqué par les éditeurs d'antivirus afin de comprendre son fonctionnement et de surtout déterminer sa signature propre. Cette signature ou encore sa carte d'identité est chargé dans la base de signature de votre antivirus via sa mise à jour quotidienne. Votre antivirus est normalement programmé par défaut pour réaliser des scans hebdomadaires pour rechercher des virus dans votre ordinateur. L'antivirus compare les fichiers scannés à sa base de signatures,. si l'un fichier correspond, il est d'abord mis en quarantaine avant d'être nettoyé.
Les éditeurs d'antivirus indiquent que ce système de comparaison de signature atteindra bientôt sa limite si le nombre de nouveaux virus ne cesse de croître. En effet, à ce moment là votre antivirus sera constamment en train de scanner votre ordinateur pour arriver au bout de sa base de signatures !

Protégez vos enfants avec un logiciel de contrôle parental

Chapitre 3

Vous avez vu au chapitre précédent que le système d'exploitation Windows XP de Microsoft autorise la création de plusieurs comptes utilisateur sur votre ordinateur. Lorsqu'il souhaite utiliser le PC, chaque utilisateur ouvre un accès distinct sur l'ordinateur, avec son profil unique et son propre Bureau, son dossier Mes documents.
Les enfants ne peuvent alors ni modifier les paramètres du système, ni installer de nouveaux matériels ou logiciels, y compris la plupart des jeux, lecteurs multimédias, logiciels de téléchargement « peer-to-peer » et programmes de conversation. Pour ce faire, ils auront besoin de votre autorisation. Il faut avoir préalablement crée autant de comptes limités que de personnes utilisant l'ordinateur.
Les comptes limités ne permettent pas de modifier les propriétés de l'ordinateur. Et donc l'enfant ne risque pas d'endommager les fichiers personnels des parents ou d'installer des programmes.

Aucun logiciel ne peut garantir une sécurité totale des enfants sur Internet. Sans l'implication pleine et entière des parents, il n'y a pas de contrôle parental efficace.

Sensibilisez et expliquez à vos enfants

Internet remplace de plus en plus la télévision. Or Internet est un média interactif au contraire de la télévision. Les enfants et les adolescents peuvent accéder à toute heure à des sites pouvant contenir des images crues voire choquantes. Ils peuvent dialoguer et interagir en direct avec d'autres Internautes sans qu'ils puissent s'assurer de leur identité. Il est donc très important que les parents expliquent et sensibilisent leurs enfants aux dangers possibles pouvant arriver sur Internet.

CHAPITRE 3

Installez et paramétrez un logiciel de contrôle parental

L'installation d'un logiciel de contrôle parental s'effectue très simplement. C'est le paramétrage qui est un peu plus difficile. Suivant l'âge de l'enfant et le type de logiciel de contrôle parental, vous pourrez agir sur plus ou moins de paramètre comme les programmes que l'enfant peut utiliser, les plages horaire où il peut accéder à Internet ou à ouvrir une session sur l'ordinateur. Vous ajusterez ensuite les paramètres par la suite pour débloquer certaines situations délicates avec votre enfant. Concernant la navigation sur Internet le principe de fonctionnement est simple : on peut, soit interdire l'accès aux sites dont l'adresse est répertoriée sur une liste noire, soit refuser les adresses ou les contenus comportant des mots indésirables ou ne permettre l'accès qu'à certains sites dont les adresses sont répertoriées dans une liste blanche. La performance du filtrage par liste noire est liée à la pertinence des sites Internet indésirables répertoriés et à la fréquence des mises à jour. De son côté, le filtrage par mots clés présente l'inconvénient de bloquer l'accès à des sites dont le contenu n'est en rien préjudiciable. Par exemple, une demande de filtrage fondée sur le mot « sein » pourra bloquer l'accès à des sites médicaux ou aux pages contenant l'expression « en son sein ». Enfin, le filtrage par liste blanche restreint considérablement l'accès à l'Internet, la consultation des seuls sites identifiés par les parents étant autorisée.
Il est à noter que le système d'exploitation VISTA de Microsoft inclu en standard un logiciel de contrôle parental.

Surveillez vos enfants

Placer l'ordinateur dans le salon afin de surveiller discrètement vos enfants sur l'utilisation qu'ils font de l'ordinateur. Vous pouvez consulter l'historique de navigation d'Internet Explorer ou de Firefox afin de surveiller les sites web visités par vos enfants. L'objectif étant toujours d'expliquer à l'enfant ce qu'il ne faut pas faire sur Internet ainsi que les risques encourus. Les logiciels de contrôle parental disposent parfois d'un outil d'enregistrement des actions faites par l'enfant sur l'ordinateur ou dans l'utilisation du navigateur Internet.

La messagerie instantanée ou "tchat"

Les jeunes et moins jeunes sont très friands de ces logiciels qui permettent de discuter en direct à travers Internet avec leurs camarades ou même avec des inconnus. Le problème de ce type de logiciels, c'est que des personnes mal intentionnés arrivent à se faire passer pour l'un de ses amis et lui demande de télécharger une photo soit disant humoristique. Cette photo est infectée par un virus ! En plus de ce problème de sécurité, il convient de faire attention aux informations personnelles, appelé profil, qui sont visibles par les personnes avec lesquelles votre enfant discute : des adultes peu scrupuleux peuvent essayer d'entrer en contact avec l'enfant en se faisant passer pour un camarade de son âge. N'indiquez aucune adresse, numéro de téléphone ou le vrai nom de votre enfant, utilisez toujours un pseudonyme. Vous avez la possibilité d'enregistrer les conversations éhangées sur MSN ou Windows Live Messenger, cela vous permettra, pour les plus inquiets d'entre vous, de vous rassurer sur les conversations et les interlocuteurs de votre enfant.

Sites internet utiles

www.security4kids.ch/FR/site/default.htm site Suisse de sensibilisation en français très bien fait.
www.filtra.info réalise tous les 6 mois des tests comparatifs sur des logiciels de contrôle parental gratuits ou payants à consulter pour choisir un logiciel efficace
www.protegetonordi.com/default.html sensibilisation à la sécurité pour les enfants et les parents
www.logprotect.fr/ logiciel gratuit de contrôle parental
www.actioninnocence.org/
www.fosi.org/ Family Online Safety Institute site en anglais. Dans la section "parents" vous trouverez des liens vers d'autres sites Internet en relation avec la protection des enfants sur Internet en plusieurs langues dont le français pour certains des sites indiqués.

Eliminez virus, mouchards et spams de votre ordinateur

Chapitre 4

La désinfection d'un ordinateur n'est pas une tâche aisée. Cela vient du fait que le système d'exploitation Windows utilise des milliers de fichiers pour fonctionner. Le but des concepteurs de virus et autres spywares est que leurs programmes malveillants restent le plus longtemps possible dans votre ordinateur.

Ils font donc le nécessaire pour s'infiltrer au cœur de votre système d'exploitation. Certains de ces programmes malveillants appelés rootkit s'installent au plus profond du système et sont quasiment indétectables. D'autres, une fois installés dans le système, désactivent l'antivirus et empêchent l'accès à la mise à jour de Windows ainsi qu'à certains sites Internet de désinfection !

La règle de base est de se méfier et de ne pas faire confiance aveuglément à son antivirus.

Note Tous les programmes du type antivirus, antispyware, contrôle parental, antispam ont besoin d'être mis à jour régulièrement étant donné le nombre de programmes malicieux se créant tous les jours à travers le monde. Cette mise à jour est réalisée automatiquement par la majorité de ces programmes.

Bien sûr l'antispam se connecte sur les sites répertoriant les adresses email des expéditeurs de spams.

Le logiciel de contrôle parental quand à lui se connecte à un site Internet indiquant les sites web inappropriés pour les enfants

Désinfecter son ordinateur

Avant de désinfecter son ordinateur, il faut déterminer s'il est ou non victime d'une attaque virale ou s'il s'agit d'un autre problème touchant à la stabilité ou à la maintenance du système (fichiers fragmentés, résidus dans la base de registre, problème matériel...) Sans un spécialiste à vos côtés, il vous sera difficile de le déterminer. Supposons dans notre cas, que votre ordinateur est infecté.
Pour pouvoir désinfecter votre ordinateur, vous devez avoir nettoyé et défragmenté préalablement votre ordinateur comme indiqué au deuxième chapitre. Cela afin de diminuer le nombre de fichiers à analyser ainsi que le temps d'analyse de l'antivirus et de l'antispyware.
Télécharger le logiciel très efficace Spybot et installez-le. Veillez à mettre à jour Spybot avant de lancer une analyse de votre ordinateur.

Lancez une analyse ou scan de votre ordinateur avec Spybot en cliquant sur le bouton "VERIFIER TOUT". Cela va prendre un certain temps en fonction de la rapidité de votre ordinateur et du nombre de fichiers à scanner.
Lancez ensuite une analyse par votre logiciel antivirus. Vous devrez normalement avoir résolu un certain nombre de problèmes. Si ce n'est pas le cas, le problème est beaucoup plus sérieux, envisagez de consulter un spécialiste du dépannage informatique à domicile tel que www.services-pc.net ou de demander de l'aide sur des forums informatiques. Si vous n'arrivez pas à accéder à Internet essayer d'utiliser l'ordinateur d'un ami et demandez de l'aide sur les forums (nécessite beaucoup de temps et de patience pour un néophyte).
Si vous pouvez accéder à Internet, certains sites proposent des « antivirus en ligne » comme www.innoculer.com Le principe est le suivant : un petit programme informatique se charge dans votre navigateur Internet qui fait alors office d'antivirus.
Vous n'avez plus qu'à lancer un scan de votre ordinateur. Cela permet de scanner sont ordinateur dans le cas où l'antivirus à été corrompu ou désactivé par le virus.

Il faut savoir qu'un ordinateur peut facilement "héberger" des dizaines voir des centaines de programes malicieux différents suivant son degré d'infection. En effet, les programmes malicieux se décomposent parfois en 2 parties. La première partie s'infiltre dans votre ordinateur généralement en profitant d'une faille de votre navigateur Internet. Elle télécharge ensuite automatiquement la seconde partie la partie "utile" de l'infection qui va permettre par exemple d'envoyer des spams à partir de votre ordinateur.

Comment éviter les virus et mouchards informatiques ?

Si vous suivez à la lettre les indications simples de ce guide, vous pouvez sans trop de difficultés surfer en toute sécurité. Ne vous éloignez pas des sentiers battus. Télécharger Firefox, un navigateur libre et gratuit concurrent d'Internet Explorer et beaucoup plus sécurisé. La dernière version de Firefox (version 3) vient de sortir (juin 2008).
Les pièges et menaces sont maintenant omniprésents, si une protection est recommandée, une attitude sensée fera la différence. Il conviendra d'éviter:
• l'utilisation de logiciels piratés, il existe des logiciels libres et gratuits qui évitent de prendre des risques et de se mettre dans l'illégalité en piratant.
• le surf sur les sites pornographiques.
• l'installation de tout logiciel/plugin sans une recherche sur sa provenance et ses effets indésirables.
• les logiciels proposés via des publicités contenues sur les sites Internet.
• les logiciels dits gratuits (une recherche avec Google sur le nom du logiciel permet d'avoir des renseignements sur les effets indésirables).
• l'exécution des fichiers reçus depuis MSN ou par email. Même si l'antivirus ne détecte rien.

A l'heure actuelle, les failles de sécurités les plus exploitées sont celles contenues sur les navigateurs Internet (surtout Internet Explorer 6), des milliers de sites Internet sont piratés en permanence. L'internaute qui tombe dessus et dont le navigateur Internet est vulnérable exécute alors automatiquement et à son insu le code malicieux, l'infection s'installe alors. Bien sûr certains sites comme les sites pornographiques ou ceux de logiciels pirates contiennent plus souvent des failles ce qui fait qu'il est risqué de s'y aventurer...
Pour pallier à cela, vous devez maintenir votre système d'exploitation à jour, ainsi que toutes les composantes (navigateur Internet, logiciels installés etc.).
• Utilisez Windows Update régulièrement. Vous pouvez configurer Windows pour télécharger automatiquement les mises à jour.
• Maintenez tous vos logiciels à jour en particulier les composants de vos navigateurs, ainsi que vos lecteurs vidéos/audio : Java, Flash, QuickTime etc. Certains logiciels critiques sont pourvus de programmes de mises à jour, utilisez-les !
• Bannissez Internet Explorer dans sa version 6, mettez à jour vers la version 7, vous pouvez aussi utiliser un navigateur alternatif comme Firefox en le sécurisant, vous échapperez aussi aux publicités sur les sites Internet.

Si un antivirus est recommandé, il ne sera jamais totalement fiable, même si sa base de signatures virales est mise à jour plusieurs fois par jour. Le sentiment de sécurité que procure un antivirus fait oublier qu'il ne faut pas faire confiance aux programmes téléchargés sur Internet.

Enfin un antivirus est destiné à la détection des virus, des trojans, des vers et backdoor. Les antivirus ne détectent ni les spywares, ni les adwares et ni les rogues. Les spécialistes de la sécurité préconisent l'utilisation de solution de sécurité complète dite "tout en un". Elle permet de protéger l'ordinateur contre la plupart des menaces connues y compris les spywares et adwares.

Les antispywares sont les programmes qui protègent contre les spywares et adwares (et parfois les rogues). Les antispywares ont un fonctionnement assez similaire aux antivirus puisqu'ils intègrent une définition virale. Cependant, les antispywares intègrent souvent une protection (minimale) contre les modifications du système, par exemple l'ajout de programmes au démarrage de Windows, la protection contre les modifications du navigateur internet etc…

Tout comme les antivirus, les antispywares sont à l'heure actuelle une protection indispensable mais ne sont pas infaillibles contre les menaces grandissantes que sont les adwares et les rogues. Il est alors nécessaire dans ce cas de faire des opérations manuelles complexes dans le système voir en dernier recours à la réinstallation complète de Windows (Réinitialisation d'usine de l'ordinateur).

Limites des antivirus et antispywares

Les limites des antivirus et antispywares se font de plus en plus sentir. S'il y a quelques années, les auteurs de virus étaient des ados qui envoyaient des vers de messageries, les auteurs de malwares sont maintenant des bandes organisées motivées par l'appât du gain.
Les technologies utilisées par les auteurs de malwares sont de plus en plus pointues, le nombre de nouvelles menaces augmente chaque jour afin que les éditeurs de logiciels de sécurité ne puissent suivre la cadence.
Le but des auteurs de malwares à l'heure actuelle est d'asphyxier de nouvelles menaces les éditeurs de sécurité pour toucher l'internaute. Les voies de propagation pour toucher l'internaute étant de plus en plus facile (Emule, pages MySpace infectées, MSN etc.).

Les antivirus/antispywares étant le dernier rempart entre les menaces et votre ordinateur, la réaction des internautes perdus est en général de multiplier le nombre de logiciels de protections, on voit parfois deux antivirus, ou 3 4 antispywares sur un même PC. Accompagnés de 3 4 barres d'outils qui ont les mêmes fonctions, on constate alors de plus en plus de sujets sur les forums: "mon ordinateur est lent", "je rame".
Il est inutile de multiplier les programmes antivirus dans un même ordinateur vous ne feriez que diminuer les performances et de rendre inefficace la détection des virus ! Il vous faut soit utiliser une solution de sécurité complète intégrant un antivirus, un pare-feu et un antispyware soit acquérir individuellement ces outils tous disponibles gratuitement sur Internet.

Quelle est la bonne réaction face aux menaces grandissantes ?

La différence se fera sur de bonnes habitudes et un minimum de méfiance. Il est clair qu'a antivirus équivalent, une personne qui télécharge sur Emule, ouvre sans réfléchir les fichiers qu'on lui propose sur MSN ou sur des publicités sera infectée contrairement à une personne qui se contente de lire ses mails.

Pour beaucoup, sécurité rime avec installation du "meilleur" antivirus et antispyware, en cinq minutes chrono on installe les plus répandus/connus et en avant: On va piller Emule, installer et essayer n'importe quel logiciel, ou ouvrir tous les fichiers qui se présentent en pensant que l'antivirus va détecter le problème et le résoudre. La sécurité est en amont, se tenir au courant, faire attention à ce que vous faites sur la toile, un utilisateur averti vaut tous les antivirus.

Comment éviter les spams ou pourriels ?

Les spams sont ce que l'on appelle des emails non sollicités. Ils sont non sollicités car ce sont souvent des emails publicitaires venant du monde entier et on ne vous a pas demandé votre avis avant de vous les envoyer. Bien souvent ces emails publicitaires vantent les mérites de la fameuse pilule bleue (viagra) ou pire de drogues ou autres appareils d'élongation du pénis ! Et encore on ne parle pas des messages vous demandant de récupérer des sommes d'argent à l'étranger ou des messages vous proposant des logiciels piratés. Pourquoi autant d'acharnement de la part de ces publicitaires ? Tout d'abord, la plupart de ces sois disant publicitaires utilisent les services de « botnet » pour envoyer des centaines de milliers de spams chaque jour. Le coût de ce genre de méthode est pour eux très compétitif étant donné qu'il suffit qu'un 1% de personnes soient dupés et achètent pour qu'ils rentrent dans leurs frais et fassent même des bénéfices ! Le fait est qu'ils profitent de la crédulité des internautes pour arriver à leurs fins. Heureusement la plupart des messages envoyés sont en anglais ou dans un français très approximatif donc facilement identifiable.
En France, la loi impose que l'expéditeur demande votre autorisation avant d'enregistrer votre adresse personnelle dans son fichier. En outre l'email publicitaire doit vous proposer de vous désinscrire du fichier si vous ne souhaitez plus recevoir de messages.
Un email peut être facilement falsifié, l'adresse de l'expéditeur est modifiée de telle façon que vous n'arriverez jamais à connaître l'identité exacte du spammeur.
Les spams sont véritablement le fléau de la messagerie sur Internet puisque 99% des emails échangés dans le monde sont des spams ! Dans ce cas vous aurez beaucoup de mal à les éviter.
Rassurez vous il existe néanmoins quelques astuces pour vous en prémunir.
1) utilisez 2 boîtes email, l'une personnelle que vous ne donnerez qu'à vos connaissances et l'autre que l'on appellera « poubelle » que vous donnerez à tous les sites Internet nécessitant une adresse email. Vous consulterez ensuite plus souvent la première boîte email que la deuxième.
2) si vous utilisez le « webmail » de votre fournisseur d'accès à internet pour consulter vos messages, vous devez disposer certainement d'un filtre antispam. Dans ce cas c'est le FAI qui s'occupe pour vous de déterminer si un email est un spam ou non. Il déplace ensuite automatiquement les messages considérés comme du spam vers un dossier spécifique nommé « indésirables »
3) si vous utilisez un logiciel de messagerie type Outlook Express ou Thunderbird, vous devez lui adjoindre un programme de filtrage du type spamfighter. Il en existe 2 types : le premier type s'intègre complètement au logiciel de messagerie, c'est le plus simple à configurer. Le second type s'intercale entre le logiciel de messagerie et Internet. Il intercepte alors les messages et vérifie ensuite s'il s'agit d'un spam ou non. Les messages considérés comme du spam sont « marqués » spam dans l'objet du message. Il suffit alors de créer une règle de tri dans votre logiciel de messagerie pour déplacer automatiquement les spams vers un dossier spécifique.

Comment font-ils pour récupérer votre adresse email ?

Si vous laissez votre adresse email sur les chats, forums, listes de diffusion, annuaires ou sites web vous courrez le risque de voir votre adresse email « aspirée » par des robots qui parcourent le web à la recherche d'adresse email. Une fois aspirée votre adresse rejoindra les fichiers des spammeurs. Une fois dans leur fichier il est quasiment impossible d'en sortir. La seule solution est de créer une autre adresse email et de la communiquer rapidement à vos correspondants. Lorsque que vous donnez votre adresse à un site Internet, vérifiez bien qu'il a mis en place une politique de confidentialité comme la loi le lui oblige. Il doit vous indiquer ce qu'il compte faire de votre adresse : il peut très bien la revendre, avec votre accord, à d'autres entreprises. Vérifiez bien les conditions d'utilisation de vos données personnelles avant de valider l'enregistrement de vos coordonnées sur un site internet quel qu'il soit.

Sites Internet utiles

http://www.innoculer.com Site d'information et de scan en ligne avec un comparatif d'antivirus
http://www.malekal.com/ Site d'entraide pour la désinfection de votre ordinateur
http://www.safer-networking.org/fr/index.html Le site officiel de Spybot
http://www.ccleaner.com/ Utilitaire de nettoyage des fichiers temporaires
http://www.arobase.org/spam/comprendre.htm Qu'est ce que le spam ?
http://www.lavasoft.fr/ Un antispyware gratuit AdAware à utiliser conjointement avec Spybot
http://www.spamfighter.com/lang_fr/ Site de l'utilitaire antispam SpamFighter

Conclusion

Internet est devenu indispensable et deviendra de plus en plus indispensable dans un futur très proche. Tout le monde l'utilise: les entreprises, l'état, les particuliers, l'administration etc... Car il permet de simplifier les procédures, de réduire les coûts, d'accélerer les échanges d'information... C'est donc un outil versatil qui peut s'adapter à tous les cas de figure. Afin qu'il soit vraiment univrsel il faut qu'il soit accessible à tout moment et en tout lieu. C'est déjà le cas aujourdh'ui avec les forfaits mobiles avec accès Internet illimité ou les accès haut débit ADSL ou fibre optique.

Dématérialisation, identité numérique, signature numérique ces termes vous seront familier car la prochaine étape d'Internet c'est la fusion de pans entiers de l'économie et de notre société pour former un réseau unique et universel totalement imbriqué et interdépendant.

Vous comprenez maintenant que plus Internet prendra de l'importance dans nos vies plus la question de la sécurité se posera de manière cruciale. C'est pourquoi il faut que dès aujourd'hui vous soyiez conscient de l'importance de maintenir votre ordinateur à jour et de suivre les conseils de ce guide. Vous pourrez alors tirer pleinement parti d'Internet sans subir ses désagréments.

Ce guide est fait pour vous et il n'est malheureusement pas exempt de défaut, c'est pourquoi nous vous encourageons vivement à faire part de vos remarques sur notre adresse email contact@services-pc.net.

Sur ce, bon surf !