1e éd - 11/2011

Entretien et sécurisation de votre PC sous le système d'exploitation Windows

Ligue Libérale des Pensionnés asbl

1e éd - 11/2011

DE L'ORDINATEUR

TABLE DES MATIERES

COMMENT ENTRETENIR ET SÉCURISER VOTRE PC

PREAMBULE 1/2

Une fois votre ordinateur installé et connecté, il est impératif de l'entretenir, comme vous le feriez pour votre voiture pour assurer son bon fonctionnement, mais aussi de le protéger des attaques du monde extérieur.

Que vous soyez connecté ou pas, si votre ordinateur n'est pas entretenu, vous risquez de rencontrer des difficultés.

En effet, après un certain temps d'utilisation et de manipulation des différents programmes, le système s'encombre de nombreux fichiers de travail devenus inutiles et obsolètes. Sa gestion s'alourdit de plus en plus également avec la fragmentation des fichiers (sorte de multiplication du nombre de fragments de fichiers gérés par le PC). Ces deux aspects normaux et bien connus du système d'exploitation de Microsoft© finissent par altérer le bon fonctionnement du PC.

Il vous faudra donc procéder à un entretien de votre PC en effectuant quelques opérations prévues par le système mais souvent mal expliquées.

Sachez dès à présent que cet entretien n'est plus à faire à partir des versions de Windows Vista©[1] et Windows Seven©[1]. En effet Microsoft[1], sous la pression des utilisateurs, a été obligé d'inclure une procédure automatique d'entretien qui défragmente les fichiers et qui supprime les fichiers obsolètes.
Seul le bon vieux Windows XP©[1] doit être entretenu manuellement.

En outre, nous entendons souvent parler de anti-virus[1], anti-spy[1], anti-spam[1], anti-phishing[1], cookies[1], …

[1] voir glossaire

PREAMBULE 2/2

Tous ces termes étranges pour les néophytes vous indiquent déjà la nécessité de protéger votre PC contre ces maux ou « malwares ».
Non seulement ces « malwares » liés à Internet peuvent alourdir votre PC, le ralentir, provoquer des erreurs dans les programmes mais aussi vous arnaquer ou même vous obliger à réinstaller complètement le système d'exploitation de votre PC (Windows©).

Il vous est donc conseillé d'installer un logiciel (un programme) de sécurité qui regroupera au mieux toutes ces protections.

Rassurez-vous, la plupart des logiciels de sécurité (que ce soit Mc Afee©[1], Norton©[1], Kaspersky©[1], BitDefender©[1], F-secure©[1], … pour ne citer que les plus courants) comprennent déjà ces 3 types de protection et sont déjà préinstallés sur votre disque dur lors de l'achat d'un nouveau PC.
Malheureusement la gratuité ne dure que 60 à 90 jours. Passé ce délai, vous serez vivement invité à acheter une licence (un abonnement) pour une durée d'un an ou plus. Il vous reste aussi la possibilité d'installer un logiciel gratuit (sans abonnement) mais il ne couvre pas la totalité des protections. Tout dépend de l'utilisation que vous faites de votre PC.
Nous verrons plus loin quels sont les différents cas d'utilisation possibles.

Ces fiches ont donc pour objectif de vous prémunir autant que possible de tous ces désagréments et de vous aider à y voir plus clair.

[1] **voir glossaire**

I.COMMENT ENTRETENIR VOTRE PC

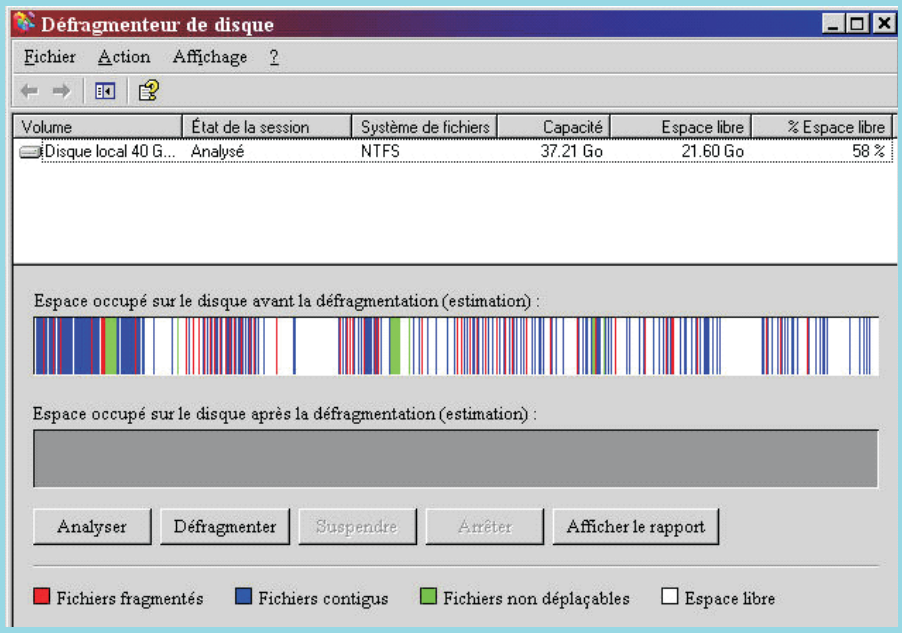
A. DEFRAGMENTATION DU DISQUE DUR

Après une utilisation même normale de votre PC, le système de dossiers et de fichiers doit être défragmenté afin de retrouver les performances qu'il avait au départ. Cette opération consiste à rassembler les nombreux fragments de chacun des fichiers et à reconstituer des fichiers uniques. Par la même occasion, les multiples espaces non utilisés (petits ou grands) mais parsemés sur le disque dur seront eux aussi rassemblés en un seul bloc.

Cette défragmentation est réalisée par un programme localisé dans les outils système. Cette opération, assez longue, se fait en arrière plan et a tendance à ralentir désagréablement le système durant toute la réalisation, elle peut même durer parfois plusieurs heures. Soyez patient et, éventuellement, ne faites rien d'autre pendant ce temps là.

PROCEDURE :
Cliquez sur : DÉMARRER, TOUS LES PROGRAMMES, ACCESSOIRES, OUTILS SYSTÈME, DÉFRAGMENTATION DU DISQUE.

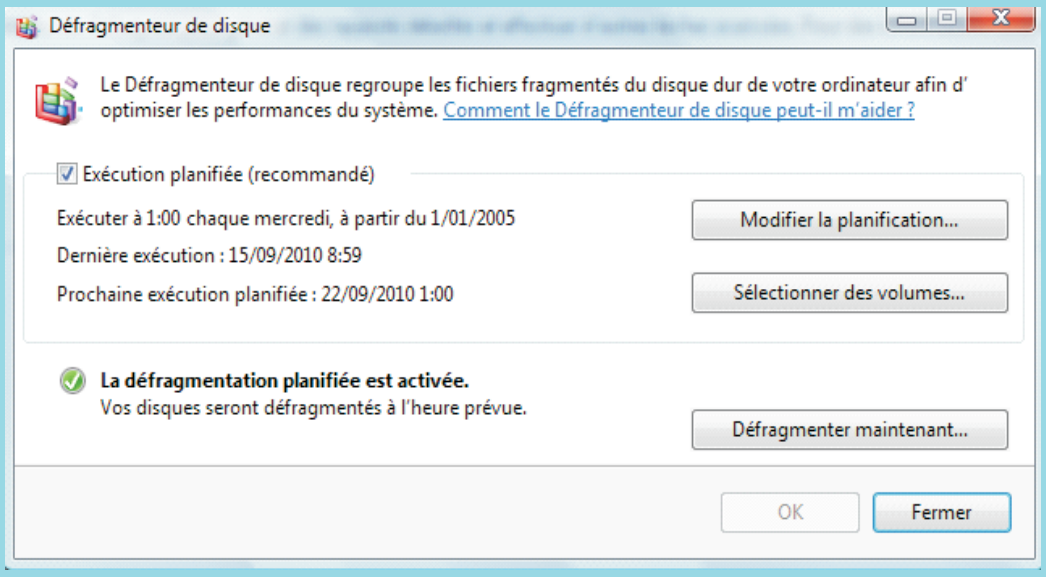
Sous Windows XP©



Sous Windows Vista / Seven©

Windows Vista© et Seven© font cette opération automatiquement.

Cependant, vous pouvez modifier la planification ou effectuer la défragmentation immédiate en cliquant sur le bouton concerné.



Par exemple, pour alléger le processus, il est conseillé de modifier la planification par défaut (par semaine) par une exécution tous les mois.
Cliquez sur : MODIFIER LA PLANIFICATION.

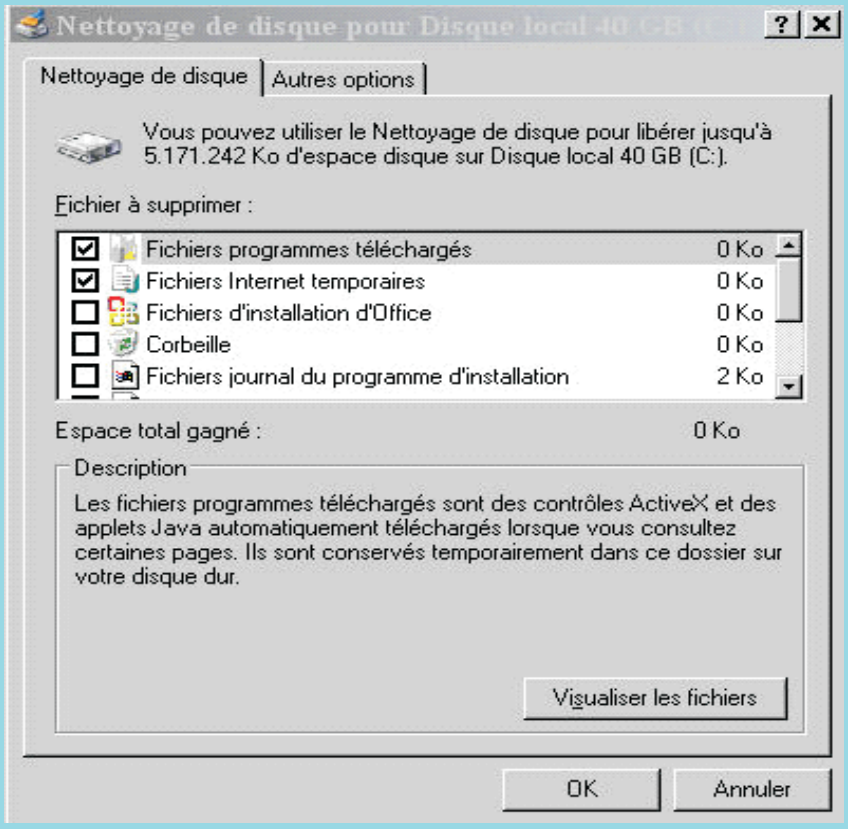
Remarque : Vous pouvez également faire appel à un logiciel externe tel que CCLEANER© téléchargeable depuis Internet et qui remplit parfaitement ces fonctions.

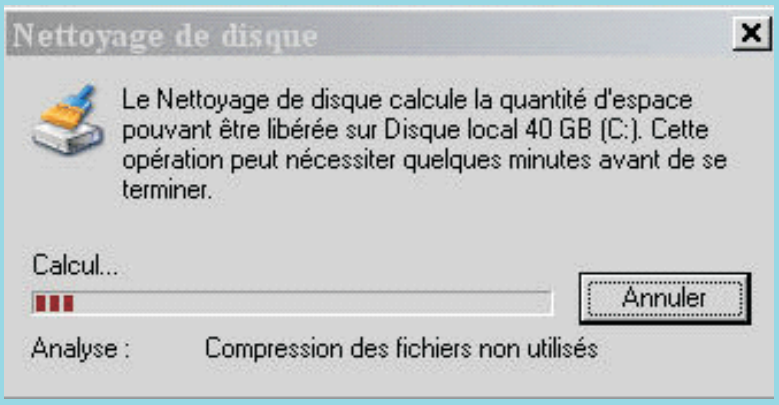
B. NETTOYAGE DES FICHIERS TEMPORAIRES DU DISQUE DUR ET DE L'HISTORIQUE DE NAVIGATION

Comme dit précédemment, le système s'encombre de nombreux fichiers de travail devenus inutiles et obsolètes. De plus, chaque fois que vous allez sur Internet, consultez un site, téléchargez, ... des données temporaires sont stockées elles aussi sur le disque dur de votre ordinateur dans l'historique de navigation. A la longue, cela peut ralentir votre système. Il faut donc le supprimer également via un programme localisé sur votre PC.

B.1. Procédure du nettoyage du disque dur

Cliquez sur : DÉMARRER, TOUS LES PROGRAMMES, ACCESSOIRES, OUTILS SYSTÈME, NETTOYAGE DU DISQUE.





NB : Décochez les postes pour lesquels vous ne désirez pas de nettoyage.

B.2. Procédure du nettoyage de l'historique de navigation

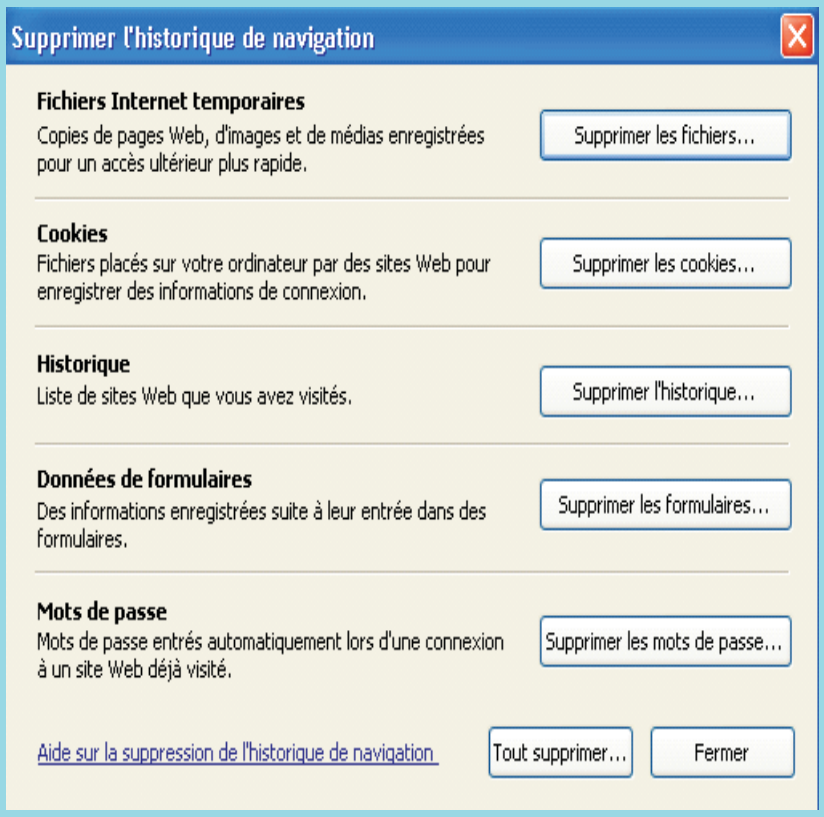
Toute votre activité sur Internet est enregistrée dans des fichiers temporaires sous forme de liens et se rassemble dans l'historique de navigation. Cet historique permet de faciliter et d'accélérer l'affichage des pages webs dernièrement consultées lors des visites ultérieures. Il permet aussi d'effectuer un contrôle parental. Mais cet historique peut devenir lourd à gérer par le pc ou même être consulté par un site Web indiscret.
Il est donc conseillé de le supprimer de votre navigateur (Internet Explorer©[1], Firefox©[1] , ...) régulièrement via la procédure ci-après.
Windows XP© n'effectue pas automatiquement cet entretien.
Par contre, Windows Vista© et Seven© le font automatiquement.

PROCEDURE :
Cliquez sur : INTERNET EXPLORER, OUTILS, SUPPRIMER L'HISTORIQUE DE NAVIGATION.

[1] **voir glossaire**

Sous Windows XP©

Cliquez sur SUPPRIMER LES FICHIERS.

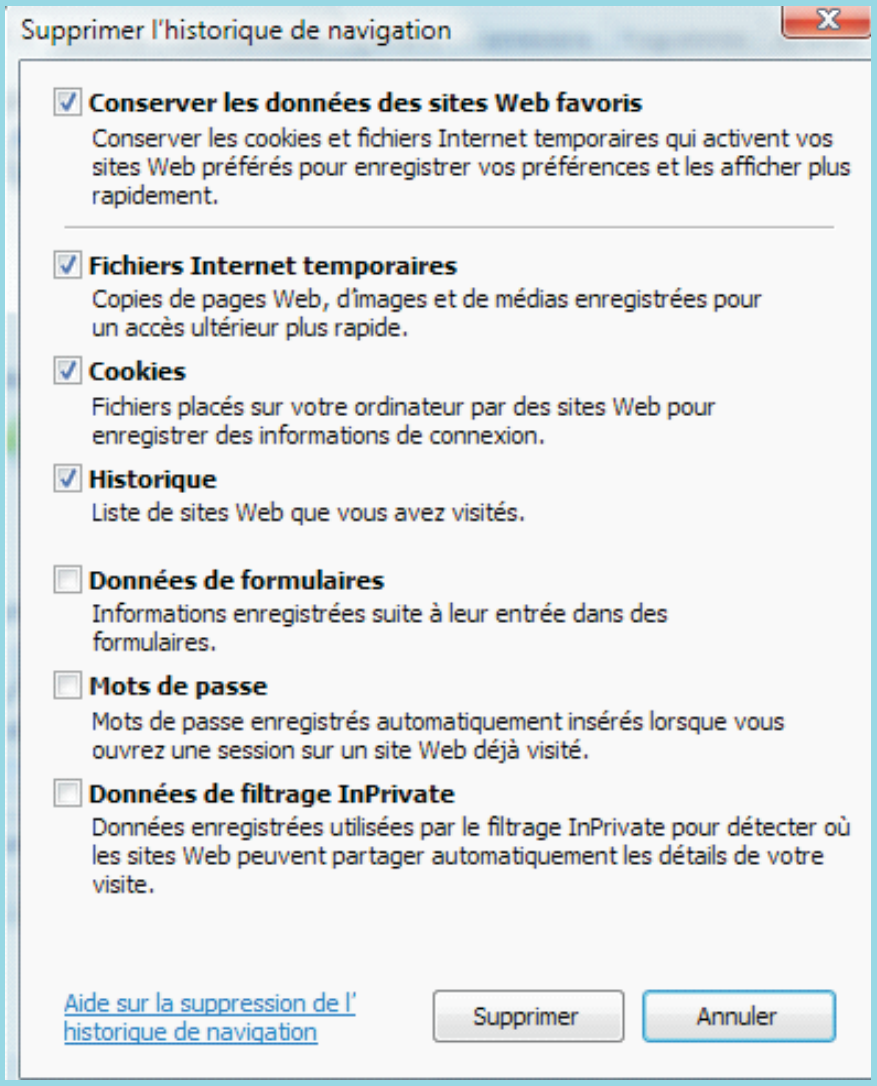


NB : vous pouvez déjà, à ce niveau, cliquer sur les autres boutons de suppression de l'historique (cookies[1], mots de passe, ...) mais pensez préalablement à noter vos mots de passe avant de les supprimer.

[1] **voir glossaire**

Sous Windows Vista / Seven©

Décochez ou cochez les cases correspondant aux suppressions désirées.



B.3. Effacer les fichiers supprimés

Aussi bizarre que cela puisse être, un fichier que vous supprimez ne l'est pas vraiment : il n'apparaît plus dans la liste, mais son contenu est toujours présent tant que d'autres fichiers n'auront pas pris sa place. Même en vidant la corbeille, il est possible de le récupérer. En fait, les fichiers sont simplement marqués pour suppression par le système et peuvent alors être "écrasés" ou remplacés par d'autres données.

Dans la pratique il n'y a pas lieu de s'inquéter puisque tôt ou tard ces fichiers sont finalement détruits par des nouveaux qui viendront s'inscrire à leur emplacement.

Sachez malgré tout qu'une défragmentation des fichiers rendra impossible la lecture des fichiers supprimés. Une défragmentation efface par définition les fichiers supprimés puisqu'elle réorganise complètement le disque dur.

Mais pour celui qui le souhaite on peut supprimer réellement ces fichiers supprimés grâce à un effaceur de fichier qui rend illisible l'espace libéré de votre disque, jardin secret riche de mille trésors anciens...

Il existe pas mal de programmes sur Internet qui réalisent ce type de nettoyage (ex : CCLEANER©).

B.4. Effacer les cookies indésirables stokés par votre Navigateur Internet[1] (Internet Explorer©[1], Firefox©[1], Chrome©[1], Opera©[1])

Les cookies sont de petits fichiers textes stockés par le navigateur Web sur le disque dur lors de vos visites sur des sites Web.
Ils servent, entre autres, à enregistrer des informations sur le visiteur ou encore sur son parcours dans le site.

En bref, les cookies peuvent ainsi reconnaître les habitudes d'un visiteur et personnaliser la présentation du site visité.

Les cookies permettent aussi de garder en mémoire, de retenir les identifiants de connexion à une éventuelle partie privée : lorsque le visiteur revient sur le site, il ne lui est plus nécessaire de taper son nom et son mot de passe pour se faire reconnaître, puisqu'ils sont automatiquement envoyés par les cookies.

[1] **voir glossaire**

Les cookies ont une durée de vie limitée, fixée par le concepteur du site. Ils peuvent aussi expirer à la fin de la session sur le site, ce qui correspond à la fermeture du navigateur.

Les cookies sont largement utilisés pour simplifier la vie des visiteurs et leur présenter des informations plus pertinentes.
Mais une technique particulière permet aussi de suivre un visiteur sur plusieurs sites et ainsi de collecter et recouper des informations très étendues sur ses habitudes.

Cette technique a donné à l'usage de cookies une réputation de technique de surveillance violant la sphère privée des visiteurs.

En pratique, pour assurer une confidentialité des cookies, il est conseillé de les supprimer régulièrement. Il existe un moyen de supprimer certains cookies et d'en conserver d'autres (par exemple pour la banque).

Pour supprimer les cookies, utilisez : soit le programme prévu par l'utilitaire Windows© "Supprimer l'historique de navigation" (voir pages 5 et 6), soit un programme d'entretien tel que CCLEANER©.

II. COMMENT SECURISER VOTRE PC

La sécurisation du PC repose sur plusieurs éléments :
- Les adresses e-mail
- Les mots de passe
- La mise à jour régulière des correctifs du système Windows© offert par Microsoft©
- La mise en place d'un logiciel de protection contre les virus, vers, espions et autres logiciels malveillants
- La protection de votre router-modem
- La protection des transactions bancaires

A. ADRESSES E-MAIL (ou courriels)

Nous ne parlerons pas ici des adresses professionnelles (ou de société) car elles appartiennent au réseau interne de l'entreprise et sont donc déjà sous protection.

Pour nos adresses privées, nous savons déjà qu'il en existe de nombreux types (Skynet©, Voo©, Base©, Mobistar©, ...). La plupart du temps, c'est le FAI[1] (Fournisseur d'Accès à Internet) qui offre 1 à 5 adresses gratuites pour chaque abonnement souscrit.
Mais vous pouvez aussi créer une adresse sur n'importe quel autre site Internet qu'il soit Google© (Gmail©), Yahoo© ou Microsoft© (Windows live mail©, Hotmail©, ...).

Toutes ces adresses sont en principe sécurisées contre les virus et malwares mais ne vous fiez pas trop à cet avantage. Nous verrons plus loin qu'un logiciel de sécurité viendra compléter ce début de protection.

En outre, il existe deux types adresses : "l'adresse mail" officielle donnée par votre FAI et "l'adresse alias" créée par l'utilisateur sur base de l'adresse officielle.
L'adresse alias permet de masquer l'adresse officielle du FAI et de la rendre plus personnelle. Il est possible de créer plusieurs adresses alias. Cependant il est nécessaire de créer l'adresse alias dans le serveur afin de pouvoir envoyer et recevoir vos mails. Si elle n'est pas créée, il ne vous sera pas possible de recevoir vos mails sur cette adresse.

[1] **voir glossaire**

1er conseil : Deux adresses mail différentes au lieu d'une seule

Afin de réduire les risques de problèmes liés au spam (publicité illicite), il est conseillé d'avoir deux adresses distinctes : une privée et une publique.
L'adresse privée sera réservée aux proches et aux amis, elle comportera souvent le nom et le prénom de la personne.
L'autre adresse sera destinée à tous les e-mails liés aux magasins et sites que vous consultez.
Dans ce cas, inventez un nom ou abréviation qui ne ressemble en aucun cas à votre identité. Sachez que des aspirateurs d'e-mail (des programmes de spam[1]) fouillent tous les médias publiques d'Internet (forums[1], newsgroups[1], sites Web[1]) à la recherche d'adresses e-mail pour se livrer au spam.
Ainsi si votre adresse publique devient polluée, vous aurez toujours une adresse e-mail privée intacte ou presque.

2ème conseil : Effacer les adresses e-mail contenues dans les mails que vous transférez à vos amis ou autres connaissances.

Lorsque vous transférez un message (blagues ou chaînes de miracles) prenez la peine d'EFFACER toutes les adresses e-mail reprises dans le message d'origine. Car, sans le savoir, vous les communiquez aux spammers[1] (expéditeurs de publicités non sollicitées).
C'est facile et très rapide : lors de votre envoi, sélectionnez le texte contenant les adresses et appuyez sur la touche SUPP ou DEL.

3ème conseil : Dans le doute, vérifier vos e-mails

Evitez de transférer des mails parlant de chaîne du malheur ou chaîne du bonheur. Il n'y a pas de petite fille qui se meurt du cancer et encore moins une fondation qui veuille l'aider en collectant des dons par l'intermédiaire d'Internet !
C'est encore un moyen pour récolter vos adresses.

[1] voir glossaire

Visitez plutôt le site www.hoaxbuster.com pour vérifier la véracité de ce type de mail.

Il suffit de taper dans la zone de recherche le ou les mots ou encore le message que vous voulez vérifier.

B. MOTS DE PASSE

B.1. Choisir un mot de passe

Le choix du mot de passe protégeant aussi bien l'accès de votre boîte e-mail que celui d'un compte ou d'un fichier est capital. Le mot de passe doit être à la fois facile à retenir pour vous et difficile, voire impossible à deviner pour les autres.

Les règles de base :
- Evitez les mots des dictionnaires et les mots inférieurs à 8 caractères
- Combinez majuscules, minuscules, chiffres et caractères spéciaux (par exemple sigles de monnaie) suivant l'intensité de sécurité que vous lui donnez
- Evitez d'utiliser le même mot de passe partout
- Créez chaque mot de passe avec votre propre méthode mnémotechnique.

Dans l'orthographe des adresses e-mail, la casse (minuscule/majuscule) n'a pas d'importance, alors qu'elle est primordiale dans les mots de passe.

Un exemple de création d'un mot de passe efficace (composé de 4 parties)

1. Un mot qui vous est strictement personnel (exemple : pouky)
2. Le nom ou abrégé du site visité (exemple : ebay)
3. Deux chiffres de votre choix (exemple : 49)
4. $

Seul le nom du site (partie 2) varie, le reste ne change pas pour vous.

Exemples :
Mot de passe pour un compte chez EBAY© serait : poukyebay49$
Mot de passe pour un compte chez HOTMAIL© serait : poukyhotmail49$
Mot de passe pour un compte chez GMAIL© serait : poukygmail49$

Non seulement, ce type de mot de passe est facile à construire et à retenir mais il est difficile à trouver par un pirate ou une personne malveillante.

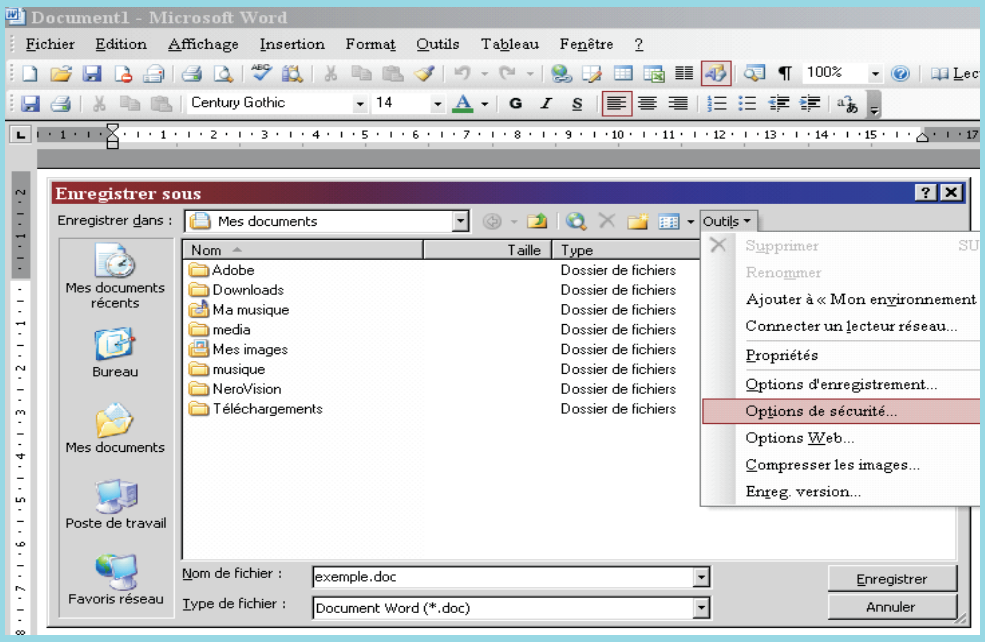
B.2. Changer de mot de passe

Les mots de passe des adresses professionnelles sont régulièrement changés avec ou sans l'accord des personnes. Le service informatique oblige ses utilisateurs à changer leur mot de passe tout en respectant les règles imposées.
Pour les adresses privées, il n'y a pas d'obligation mais il est conseillé de changer les mots de passe importants, surtout lorsque vous soupçonnez des irrégularités dans votre courrier. Même si le pirate a trouvé un filon pour intercepter votre mot de passe, si vous en changez il devra à nouveau courir un risque.
Par contre, changer de mot de passe trop souvent n'est pas une bonne solution non plus. En changeant souvent, vous risquez la confusion ou l'oubli. On note le mot de passe sur un papier qui risque de traîner n'importe où ou encore on l'enregistre sur son ordinateur, ce qui à terme baisse fatalement le niveau de sécurité.
Il vaut donc mieux changer votre mot de passe dès qu'un accès vous paraît anormal et prévenir alors votre FAI[1] (par exemple Telenet©, Skynet©, ...).

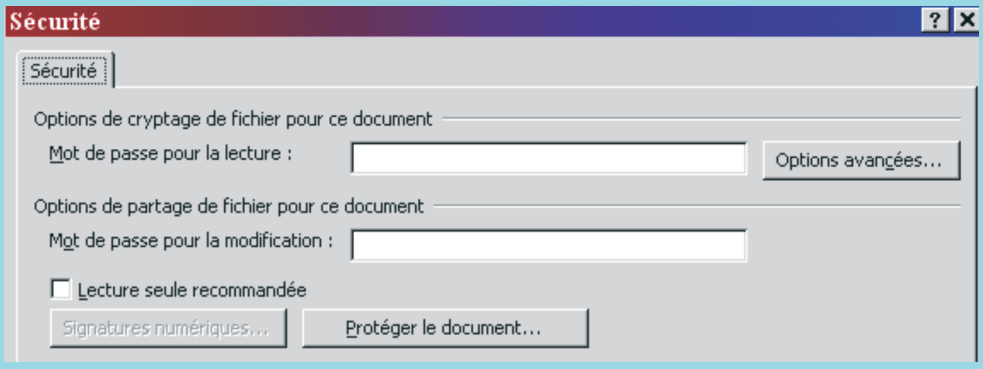
Une autre façon de retenir vos mots de passe est de les stocker dans un fichier Word qui lui est verrouillé par un mot de passe unique bien connu de vous-même et invariable.

PROCEDURE :

1) Cliquez sur : FICHIER, ENREGISTRER SOUS, OPTION DE SÉCURITÉ



2) Tapez votre mot de passe (Attention ! A retenir car il sera quasi impossible de le retrouver). Cliquez sur ok.



C. MISE A JOUR DES CORRECTIFS DU SYSTEME D'EXPLOITATION WINDOWS©

Régulièrement, des pirates essaient de s'introduire dans le système en exploitant les failles du Windows©. Grâce aux correctifs (Service Pack) gratuits envoyés par Microsoft©, vous pouvez protéger votre système d'exploitation (Windows©) et votre navigateur Internet (Internet Explorer©[1]).

Ces correctifs de sécurité sont régulièrement publiés sur le site de l'éditeur de votre système d'exploitation.

Des mises à jour ou nouvelles versions sont également disponibles et téléchargeables. Vous pouvez aussi demander à votre PC d'effectuer ces mises à jour et correctifs proposés soit automatiquement soit manuellement.
Le mode automatique (exécuté par défaut lors de l'installation) ralentit parfois fortement le système lors des téléchargements et alourdit Windows inutilement.

Il faut savoir que cette opération peut se faire en plusieurs étapes :

1. Au démarrage et sans que vous le sachiez le système se connecte à Internet et commence le téléchargement (phase parfois longue)
2. Il installe ensuite les correctifs et ce, toujours en arrière plan
3. Si il y a lieu, il impose une mise à jour supplémentaire lors de la fermeture du système. Dans ce cas, un message vous avertira de ne pas éteindre le PC car il s'en chargera lui-même.

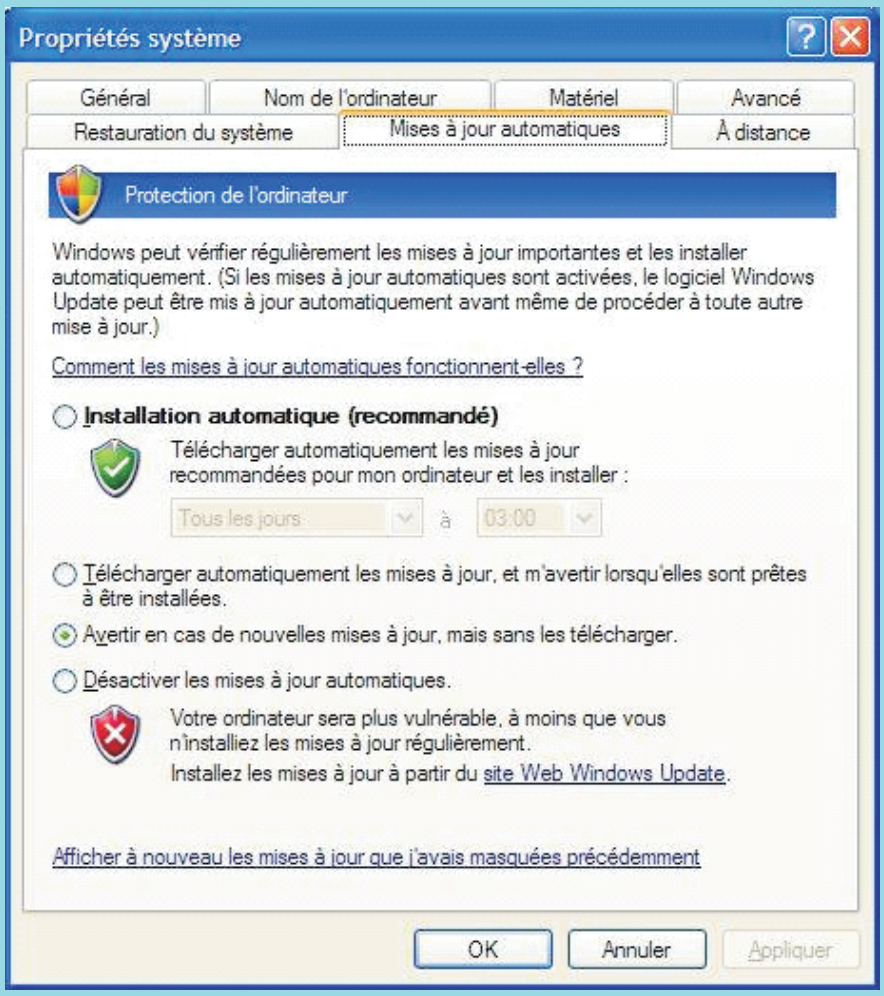
Le mode manuel (réservé aux utilisateurs avertis) permet de télécharger "à la demande", de personnaliser et sélectionner seulement les différentes mises à jour à implanter ou non dans le système.

[1] **voir glossaire**

PROCEDURE :

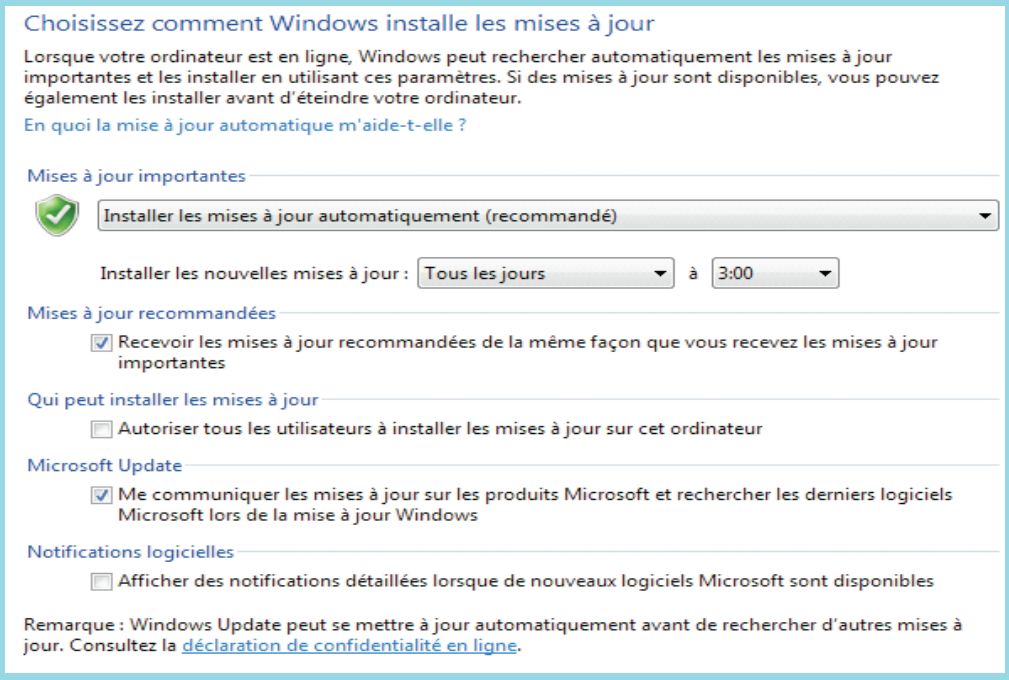
Sous Windows XP© :

Cliquez sur : DÉMARRER, PANNEAU DE CONFIGURATION, MISE À JOUR AUTOMATIQUE, cocher ou décocher l'option choisie



Pour les utilisateurs avertis, vous pouvez décocher l'installation automatique mise par défaut lors de l'installation. Et cocher l'option "Avertir en cas de nouvelles mises à jour...".
Vous aurez alors la possibilité de les installer quand vous le souhaiterez.

Sous Vista / Seven© :
Cliquez sur : DÉMARRER, PANNEAU DE CONFIGURATION, WINDOWS UPDATE, MODIFIER LES PARAMÈTRES.



D. LOGICIELS DE PROTECTION : anti-virus[1], fire-wall[1], anti-spy[1], anti-spam[1], anti-worm[1]

D.1. Virus et Anti-virus

Un virus informatique est un programme informatique créé dans le but de nuire et d'entraver le fonctionnement des PC, des réseaux et des logiciels.
Les virus peuvent se cacher dans de simples fichiers (photos, musique, films, ...). Ils se logent dans d'autres logiciels ou programmes apparemment inoffensifs. Une des méthodes bien connue est le "cheval de Troie" faisant référence à la stratégie utilisée par un cheval de bois pour conquérir la ville de Troie.
Les virus s'introduisent assez facilement dans les PC et se développent à un moment donné, provoqué par un événement aléatoire ou déterminé.

[1] **voir glossaire**

Pour la petite histoire, il y avait 1 nouveau virus tous les 6 mois dans les années 80, il y en a plus de 10 par jour à l'heure actuelle ...!

Le principe de l'anti-virus est de détecter en permanence les virus en mémoire de travail centrale (RAM) ou ceux qui tenteraient de s'introduire dans le système. Mais il effectue également et régulièrement une analyse complète des fichiers du disque dur et/ou de tout autre support tel que CD, DVD, clé USB. Une des premières missions de votre anti-virus sera donc de télécharger les nouveaux anti-virus trouvés sur votre serveur et les inoculer dans votre PC afin de le protéger. Cette opération se fait au moment du démarrage du Windows©. Lorsqu'un virus est détecté, l'anti-virus essaiera de réparer le fichier infecté. Sinon il mettra le fichier infecté en "quarantaine" ou le supprimera définitivement. Dans ce cas il peut y avoir des conséquences fâcheuses selon que ce fichier soit important ou non pour le système. Si c'est un fichier Windows© qui est infecté, le système devient instable, se fige et c'est la panne assurée. Les fichiers mis en quarantaine sont verrouillés par l'anti-virus, ils attendront une nouvelle version capable de les désinfecter. Il existe de nombreux logiciels anti-virus dont la version de base est généralement gratuite mais il est préférable de faire l'acquisition de la version payante pour élargir le champ d'application du programme de sécurité (anti-virus[1], anti-spy[1], anti-spam[1], anti-worm[1]).

AVG©[1]**, AVAST©**[1]**, AVIRA©**[1] sont quelques exemples d'anti-virus gratuits en version de base.

AVIRA© semble le plus facile à installer et n'a pas de renouvellement de licence à faire périodiquement, ce qui est le cas pour AVAST©.

NORTON©, MC AFEE©[1]**, KASPERSKY©**[1]**, ESET©**[1]**, BULLGUARD©**[1] sont des anti-virus payants ou disponibles en versions d'essai (limitées dans le temps pendant 1, 2 ou 3 mois).

NORTON© est très connu car il est préinstallé dans la plupart des nouveaux PC. Malheureusement, il a la réputation d'être lourd et d'occuper une grande partie de la mémoire de travail (RAM).

ESET© est peu connu mais est très rapide et occupe peu de place dans la RAM.

[1] **voir glossaire**

D.2. Le firewall (pare-feu)

Le pare-feu vous protège des intrusions de l'extérieur et des tentatives de prise à distance du contrôle du PC. Il est également assuré par Windows© mais il peut l'être aussi par les anti-virus.

D.3. Spy et anti-spy (anti-espion)

Cette partie de logiciel de sécurité recherche les programmes espions cachés dans votre PC qui pourraient lire certaines informations (cookies, coordonnées, adresse e-mail, sites visités, centres d'intérêt, ...) pour vous envoyer de la pub ciblée et non sollicitée. Certains logiciels malfaisants tels que les "Keyloggers" installés par un virus de type "cheval de Troie", peuvent même enregistrer vos frappes au clavier, en particulier vos pseudonyme et mot de passe, pour les envoyer ensuite à un pirate.

D.4. Spam et anti-spam (anti-publicité)

Le spam, ou comme disent les Canadiens le "pourriel," est une communication électronique non sollicitée via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.

D.5. Worm et anti-worm (anti-ver)

Les vers actuels se propagent principalement via les fichiers attachés de la messagerie (et notamment par le client de messagerie Outlook©) Ces fichiers attachés contiennent des instructions permettant de récupérer l'ensemble de votre carnet d'adresses et d'envoyer des copies d'eux-mêmes à tous ces destinataires.

Tous ces problèmes font peur mais, fort heureusement, la plupart des principaux locigiels de sécurité cités plus haut (les payants) assurent toutes ces protections plus ou moins bien.

Il existe aussi des programmes spécifiques qui assurent séparément la protection anti-malware[1] des anti-virus traditionnels (ex : malwarebyte via Internet).

E. PROTECTION DE VOTRE ROUTER-MODEM

La protection du router-modem par un mot de passe autre que celui fourni par défaut est vivement conseillé. En pratique la plupart des constructeurs ont donné des mots de passe trop simples (ex : admin, 1234, ...).
Cela laisse la porte ouverte aux pirates.

Procédure:
Lancez Internet Explorer (ou un autre navigateur),tapez 192.168.1.1 (pour les routers Belgacom©) dans la barre d'adresse (là où vous tapez habituellement www...). Bien que tout ceci soit bien expliqué dans le guide d'installation, si vous éprouvez des difficultés, demandez à un technicien de votre FAI (Belgacom©, VOO©, ...), d'effectuer cette sécurisation supplémentaire.

De même, si vous utilisez un réseau sans fil (Wifi) , sécurisez-le avec un mot de passe très personnel. En effet si le Wifi n'est pas sécurisé une personne se trouvant dans un rayon de 20-25 mètres peut s'y connecter, profiter de votre abonnement et même s'introduire dans votre PC via le router-modem.
C'est possible via une voiture parquée devant chez vous mais c'est aussi le cas dans les endroits publics pourvus d'une connexion Internet sans fil et sans mot de passe.

Dans tous les cas "privés" le réseau Wifi devrait être sécurisé même si il y a partage de la connexion par exemple pour des étudiants en kots.

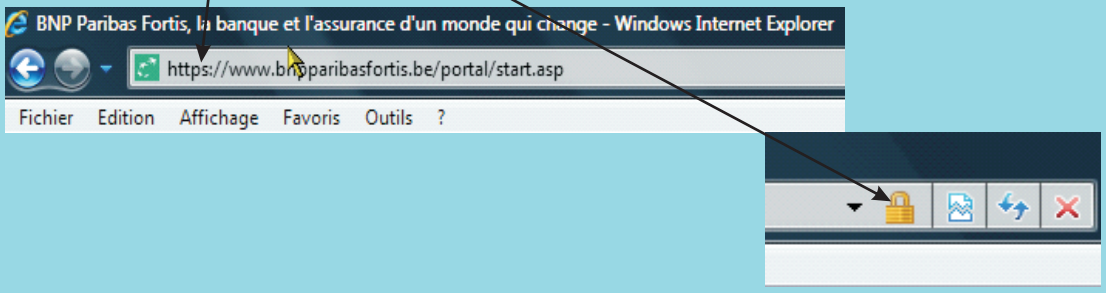
[1] **voir glossaire**

F - PROTECTION DES TRANSACTIONS BANCAIRES

F.1. //http et //https, quelle différence ?

Tous les sites Internet sécurisés doivent avoir une adresse commençant par “https”, le “S” supplémentaire indiquant un contenu sécurisé. Il s’agit d’un grand principe sans aucune exception. il doit également figurer une petit icône représentant un cadenas fermé.

Par exemple, le site de BNP Paribas Fortis : www.bnpparibasfortis.be



F.2. Filtre anti-hameçonnage ou anti-phishing

Il s’agit d’une technique de piratage qui vise à récupérer des mots de passe et soutirer de l’argent ou des informations confidentielles aux internautes par l’intermédiaire d’e-mails les orientant vers de faux sites.
Les victimes reçoivent un message qui semble “authentiquement” provenir d’une banque, d’un FAI ou de tout autre prestataire de service en ligne. Le message invite l’internaute à confirmer son code d’accès en prétextant un problème de sécurité.
Si l’internaute clique sur le lien donné dans le message, il atterrit sur un faux site qui imite de manière très précise le site de l’institution ou de l’entreprise concernée. Par défaut, le système active le filtre anti-hameçonnage[1], mais vous pouvez le désactiver vous-même et faire les vérifications quand vous le souhaitez en cliquant sur l’icone se situant en bas de l’écran de votre navigateur Internet Explorer© et étant représenté comme suit :

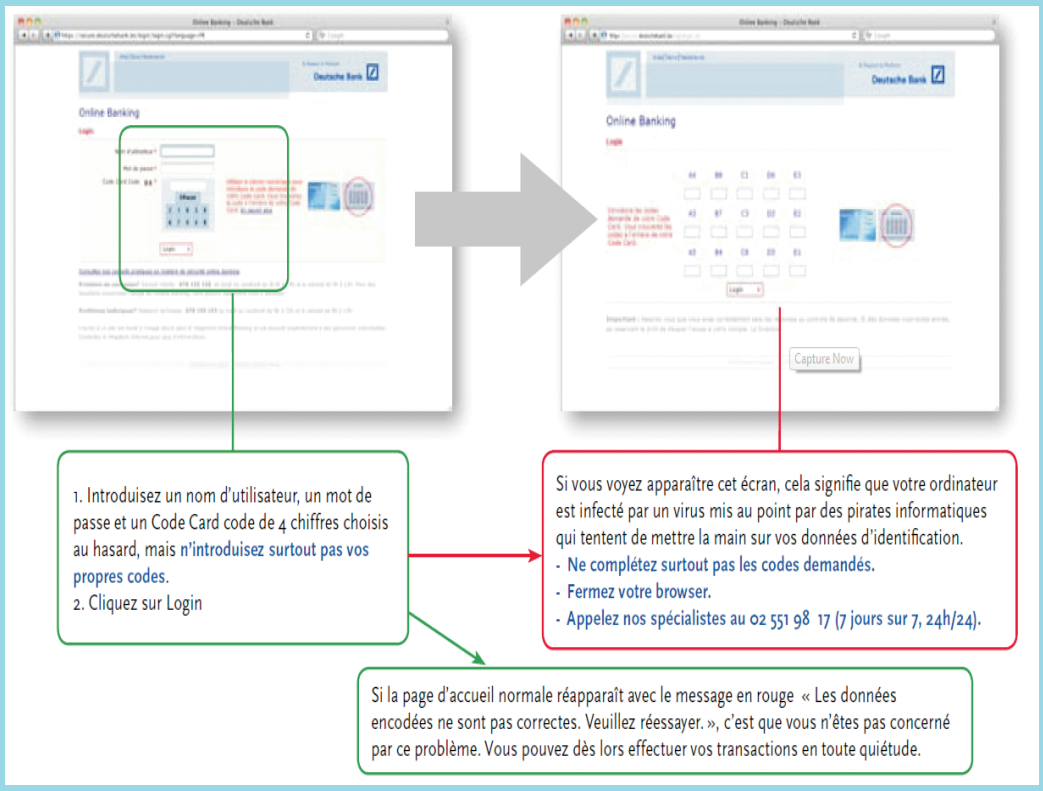
[1] **voir glossaire**

.

Quelques exemples de phishing

1) La banque “Deutsche Bank” a été victime d’une arnaque.

On remarque bien la similitude des écrans qui trompe l’utilisateur en ligne.



2) Autre exemple d'arnaque au phishing contre le site Paypal
Voici le faux message que reçoit l'internaute qui aurait un compte Paypal.
Les fautes de frappes et de grammaire devraient attirer votre attention.

"From : Service clientele <noreply.internet@orange-ftgroup.com
Date : 2009/4/19
Subject : PayPal - Attenion! D'acces frauduleuses a votre compte.

Cher client PayPal,

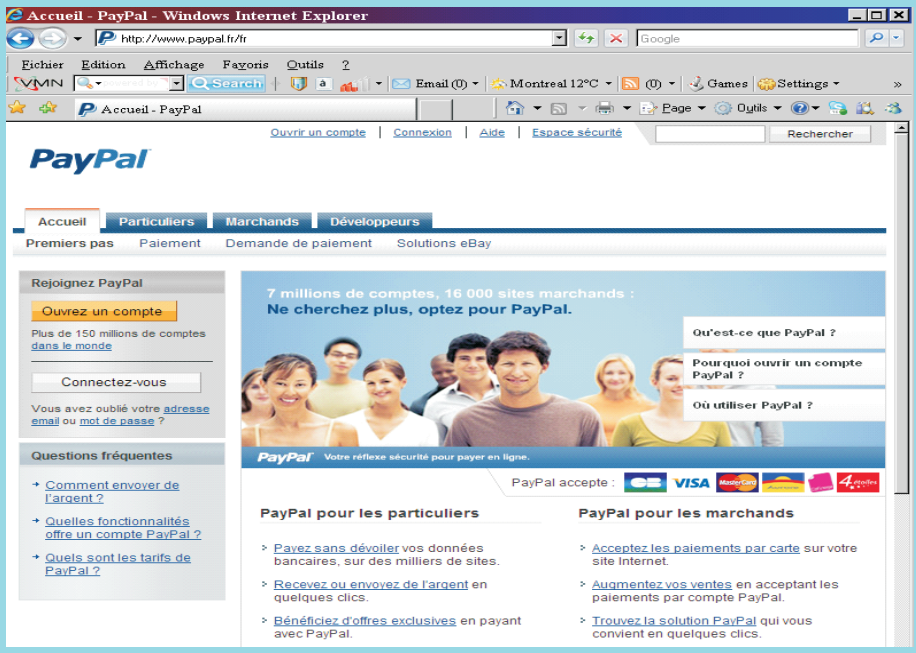
Conformément à nos mesures de sécurité, nous avons tenté de vous joindre pour une vérification de vos données, mais n y avons malheureusement pas réussi. C est le dernier rappel pour vous connecter PayPal. Une fois que vous serez connecter. PayPal vous fournira des mesures pour rétablir l'accès de votre compte.
Votre compte a peut-être été utilisé par un tiers. Nous avons restreint l'accès aux fonctions sensibles du compte Paypal, pour le cas ou il serait utilisé par une tiers non autorisé. Nous comprenons que l'accès restreint peut constituer une gêne, mais la protection de votre compte est notre priorité absolue.
Votre numéro de Référence ; FN-253-412-717
C'est le dernier rappel pour vous connecter PayPal. Une fois que vous serez connecter, suivez les tapes pour activer votre compte. Nous vous remercions de votre compréhension pendant que nous travaillons assurer la sécurité compte.
https://www.paypal.fr/fr/cgi-bin/webscr?cmd=login-submits
Nous vous remercions d'utiliser PayPal, la solution de paiement et de rception de paiement en ligne la plus simple et la plus scurise.
Cordialement
PayPal

Département Anti-Frauduleux.
Veuillez ne pas rpondre cet mail. Cette boîte aux lettres n'est pas consultee et vous ne cevez aucune reponse.
copyright 1999-2009 PayPal. Tous doits rservs.
PayPal (Europe) S. r.l. & Cie, S.C.A.
Socit en Commandit par Actions

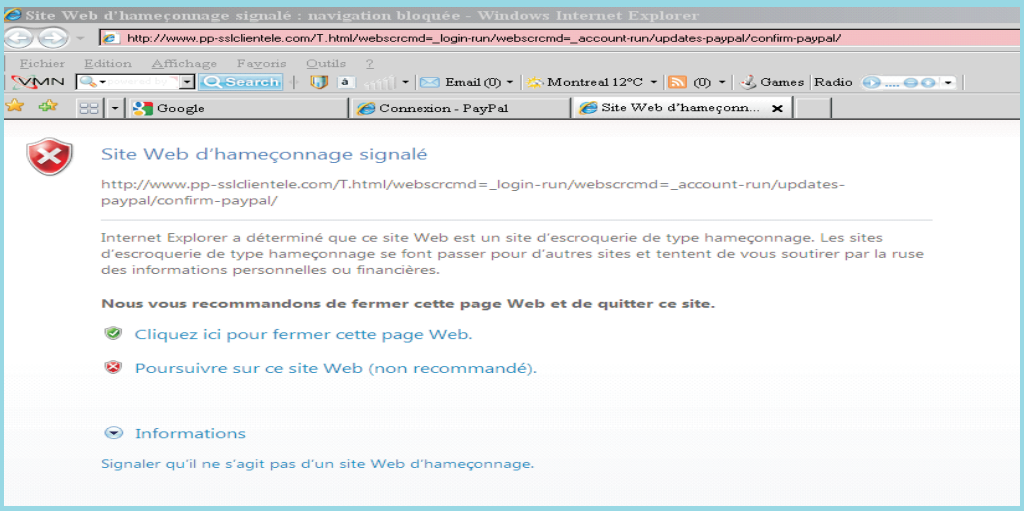
Sige social : 5me tage 22-24 Boulevard Royal L-2449, Luxembourg"
RCS Luxembourg B 118 349 Email PayPal n PP1469"

Ceci est le faux site qui invite les internautes à donner leurs codes

Ceci est le site officiel de PayPal



Et voici le blocage réalisé par le filtre anti-hameçonnage



F.3. Codes d'accès aux comptes bancaires

Les mots de passe jetables
Le système repose sur un petit appareil qui ressemble à une calculette et qui génère automatiquement des mots de passe à usage unique (comme BNP Paribas Fortis). Leur vol et leur utilisation frauduleuse deviennent impossibles.

Exemple sur www.fortisbanking.be

Une autre solution consiste à introduire certains chiffres “désordonnés” de la carte bancaire (comme la Deutche Bank).
Récemment, cette banque a abandonné son système de sécurité et a opté la calculette comme le font des banques actuelles.

Rappel : Le code généré par cette calculette est unique et rend impossible une éventuelle fraude à condition de respecter les règles de base de sécurité, d’entretenir régulièrement son pc et de la protéger en permanence.

CONCLUSION 1/2

Vous l'aurez compris, afin d'éviter de rencontrer des problèmes avec votre ordinateur, vous ne devez pas oublier de l'entretenir et de le protéger, tout comme vous le feriez pour votre voiture ou … pour vous-même.

La défragmentation et les procédures de nettoyage vous permettront d'alléger votre ordinateur et d'améliorer ses capacités de traitement.

En outre, afin de sécuriser au mieux votre ordinateur, gardez en mémoire les points suivants :

- **Ayez deux adresses e-mail et des mots de passe sécurisés ;**
- **Acceptez les mises à jour et correctifs de Windows© et Internet Explorer© ;**
- **Evitez d'installer des logiciels piratés, pour lesquels vous n'avez pas acheté de licence ; n'utilisez pas de logiciels « copiés », ils seront refusés lors des mises à jour des correctifs et seront donc vulnérables aux attaques ;**
- **Installez un bon logiciel de sécurité contre les intrusions : les virus, les spy, les spam, les vers, l'hameçonnage, … ;**
- **Soyez prudent si vous avez un fichier attaché à un mail (attachment) et que vous ne possédez pas un bon anti-virus, ne l'ouvrez pas à l'aveugle ;**

CONCLUSION 2/2

- **N'acceptez jamais d'invitation à analyser gratuitement votre PC sous prétexte que vous avez des infections ;**
- **Sécurisez l'accès à votre router-modem et l'accès à votre réseau sans fil (Wifi) ;**
- **Ne donnez jamais des renseignements ou codes personnels même si c'est la banque qui vous le demande ;**
- **Respectez bien les consignes de sécurité lorsque vous effectuez des achats sur Internet ;**

Nous espérons que ce document vous permettra de mieux vous y retrouver dans les démarches à effectuer et de gérer au mieux les soucis que vous pourriez rencontrer avec votre ordinateur quant à son entretien et sa sécurisation.

GLOSSAIRE

Anti-hameçonnage, anti-malware, anti-phishing, anti-spam, anti-spy, anti-virus, anti-worm : pour lutter contre hameçonnage, malware, phishing, spam, spy, virus, worm

Avast© : logiciel anti-virus gratuit, licence à renouveler, version payante possible

Avira© : logiciel anti-virus gratuit, licence permanente, version payante possible

AVG© : logiciel anti-virus gratuit, licence permanente, version payante possible

BitDefender© : logiciel anti- virus

Bullguard© : logiciel anti-virus payant

Ccleaner : logiciel de nettoyage

Chrome© : navigateur Internet développé par Google©

Cookies : petits fichiers textes stockés sur le disque dur de par la consultation de sites internet

Courriel : courrier électronique appelé aussi e-mail

Défragmentation : rassemblement de tous les fragments de fichiers en un seul bloc, effacement des fichiers supprimés et rassemblement des espaces libres

Eset© : logiciel anti-virus payant

FAI : Fournisseur d'Accès à Internet, c'est donc la société où vous payez les factures pour la connexion à Internet (par exemple Belgacom©, VOO©, Télénet©)

Firefox© : navigateur Internet de Mozilla©, concurrent de Microsoft©

Firewall ou pare-feu : protège des intrusions de l'extérieur et des tentatives de prise de contrôle à distance du PC

Forums : lieux de discussion via Internet

F-secure© : logiciel de sécurité

Hameçonnage ou phishing : technique utilisée par des fraudeurs pour obtenir des renseignements personnels par courrier électronique ou sites Web dans le but d'usurper une identité et de soutirer des renseignements très personnels

Internet Explorer : navigateur Internet de Microsoft©, il est installé par défaut avec Windows

Kaspersky© : logiciel anti-virus payant

Keyloggers : dispositif espion qui permet d'enregistrer les courriers électroniques consultés ou envoyés, les fichiers ouverts; permet aussi de récupérer les mots de passe des utilisateurs

Logiciel : ensemble de programmes, de données utilisés pour le bon fonctionnement du PC

Malware© : logiciel malveillant développé dans le but de nuire à un système informatique. Les virus et les vers en sont deux exemples très connus.

Mc Afee© : logiciel anti-virus payant

Microsoft© : société co-fondée par le célèbre Bill Gates qui domine depuis de nombreuses années le marché des systèmes d'exploitation tels que Windows©

Navigateur Internet : logiciel conçu pour consulter Internet.
(par exemple : Internet Explorer, Firefox©, ...)

Newsgroup : groupe de discussion sur Internet

Norton© : logiciel anti-virus payant

Opera© : navigateur Internet

Pare-feu : voir firewall

Phishing : voir hameçonnage

Pourriel : voir spam

Sites Web : sites Internet

Spammers : expéditeurs de publicités non sollicitées

Spam ou pourriel : courrier électronique publicitaire non sollicité

Spy : programme espion qui peut voler des informations à votre insu

Virus : C'est un programme informatique qui affecte ou infecte un ordinateur en modifiant la façon dont il fonctionne, sans l'autorisation de l'utilisateur. Il peut endommager sérieusement le système d'exploitation de l'ordinateur et obliger l'utilisateur à réinstaller son windows. Il peut se dupliquer et infecter d'autres ordinateurs via les envois de messagerie et ou les téléchargements depuis internet.

Wifi : réseau sans fil d'accès à Internet

Windows© : système d'exploitation de Microsoft© ; les plus récents sont le XP©, Vista© et le tout dernier Seven©

Worm ou ver : programme capable de se répliquer à travers les terminaux connectés à un réseau, puis d'exécuter certaines actions pouvant porter atteinte à l'intégrité des systèmes d'exploitation.

Ligue Libérale des Pensionnés asbl
rue de Livourne 25 - 1050 Bruxelles
TEL : 02/538.10.48 - FAX : 02/542.87.45

ligueliberaledespensionnes@mut400.be
www.ligueliberaledespensionnes.mut400.be

Avec le soutien de

Nous remercions
les membres de la commission “NTIC”
de la Ligue Libérale des Pensionnés asbl
pour leur collaboration

Editeur responsable : Mr Etchegaray - rue de Livourne 25 - 1050 Bruxelles