

Safe-Hex

L'indispensable pour Internet

Sébastien SAUVAGE
<http://www.sebsauvage.net>

Mise en page et adaptation pour l'impression par Simon Plante
<http://www.blogsimonpca.ca.cx>

1 Pourquoi sécuriser mon ordinateur, je n'ai rien à cacher !

Ne pas sécuriser votre ordinateur, c'est permettre à un inconnu d'en prendre le contrôle total, à votre insu, et d'en faire ce qu'il veut : voler vos mots de passe, se faire passer pour vous, voler vos fichiers personnels, voler votre numéro de carte bleue, utiliser votre ordinateur et votre connexion internet pour faire des choses illégales comme spammer, envoyer des virus, pirater d'autres ordinateurs, diffuser illégalement des MP3 ou des films ou encore diffuser des images pédophiles. C'est une réalité technique, c'est faisable et relativement facile.

Ne pas respecter ces règles de sécurité, c'est vous exposer à des ennuis, qui peuvent aller de la simple gêne jusqu'à des poursuites judiciaires. Ce ne sont pas des légendes urbaines, un certain nombre d'internautes ont déjà eu affaire à la justice. C'est une réalité : vous êtes légalement responsable de ce qui est fait à travers votre connexion internet. Dans le cyberspace, vous n'êtes pas anonyme. Votre fournisseur d'accès sait qui vous êtes et peut fournir votre identité aux autorités si nécessaire. Les pirates peuvent utiliser votre ordinateur comme relai : Du point de vue de votre fournisseur d'accès internet, c'est vous qui aurez effectué ces actions, et c'est vous qui serez tenu pour responsable.

Ne pas sécuriser votre ordinateur, ça vous est préjudiciable, et c'est préjudiciable aux autres.

2 Comment faire ?

Voici le strict minimum pour internet. Toute personne avec Windows et internet devrait suivre ces règles.

WindowsUpdate + AntiVirus + Firewall + AntiSpyware

WindowsUpdate est gratuit pour tout le monde, et vous pouvez obtenir des antivirus, anti-spywares et firewalls gratuitement. Je vous recommande :

- l'antivirus Avast! Home Edition :
<http://sebsauvage.net/logiciels/fprot.html#avast>
 - le firewall ZoneAlarm :
<http://sebsauvage.net/logiciels/zal.html>
 - les antispywares Spybot Search & Destroy et Ad-Aware :
<http://sebsauvage.net/logiciels/spybotsd.html>
- Et enfin :

N'UTILISEZ PLUS INTERNET EXPLORER.

Utiliser ce navigateur est dangereux et peut permettre à des pirates, virus, spywares (et tout un tas d'autres saletés) d'entrer dans votre ordinateur. Des failles de sécurité importantes sont régulièrement découvertes, que Microsoft met parfois plusieurs mois à corriger. Utilisez de préférence Firefox, plus sûr et plus pratique (voir <http://sebsauvage.net/logiciels/firefox.html>).

Faites de Firefox votre navigateur par défaut, mais conservez Internet Explorer : il est obligatoire pour WindowsUpdate

2.1 WindowsUpdate : Je lance régulièrement WindowsUpdate et j'installe toutes les mises à jour critiques

Pourquoi ?

Régulièrement, des failles (des erreurs de programmation) sont découvertes dans Windows et ses logiciels (Internet Explorer, Outlook Express...). Ces erreurs sont exploitées par des virus ou des pirates pour pénétrer dans votre ordinateur.

Généralement, au bout de quelques semaines, voir quelques jours, apparaît un virus capable d'exploiter une faille récemment découverte.

Il est donc important de les corriger.

Comment ?

Windows est fourni avec WindowsUpdate , un programme qui permet de détecter automatiquement les failles connues dans votre ordinateur et qui va télécharger et installer automatiquement les correctifs fournis par Microsoft.

Pour cela :

- Lancez Internet Explorer
- Allez sur <http://windowsupdate.microsoft.com>
- Cliquez sur « Rechercher des mises à jour », et attendez un peu.
- Sélectionnez toutes les mises à jour critiques et cliquez sur « Installer maintenant ». (Il est possible que vous ayez à redémarrer votre ordinateur plusieurs fois à la suite de ceci.)
- Revenez sur <http://windowsupdate.microsoft.com> jusqu'à ce qu'il n'y ait plus de mise à jour critique à installer.

C'est terminé!

Notes

- Vous n'êtes pas obligé d'installer les mises à jour non-critiques. Elles sont optionnelles.
- Je vous recommande :
 - soit de faire un WindowsUpdate toutes les semaines (voir plus, si c'est possible).
 - soit de vous tenir au courant de l'actualité en matière de sécurité et lancer WindowsUpdate quand c'est nécessaire.
 - soit d'activer le lancement automatique de WindowsUpdate (cette option n'est pas disponible dans toutes les versions de Windows).
- Notez que WindowsUpdate n'est plus disponible pour Windows 95. Il ne sera disponible pour Windows 98 et NT4 que jusqu'en 2006.

2.2 Antivirus : J'ai un antivirus installé et il est mis à jour régulièrement

Pourquoi ?

On estime qu'il existe plus de 60000 virus différents. Il suffit d'un seul fichier pour être infecté et votre ordinateur en comporte des milliers. Il est humainement impossible de connaître tout ces virus, de passer en revue chaque fichier ou de connaître toutes les failles de vos logiciels qui pourraient permettre l'introduction d'un virus.

Comment ?

C'est là que les antivirus interviennent : ils connaissent ces virus et sont capables de les détecter dans les fichiers, de les neutraliser et dans certains cas de désinfecter les fichiers.

Certains antivirus sont même capables de scanner automatiquement le moindre fichier que vous utilisez : Vous n'avez plus à explicitement demander à l'antivirus de 'scanner' (vérifier) tel ou tel fichier. Ainsi quand vous lancez un jeu, l'antivirus va 'scanner' le jeu avant de vous laisser jouer. Quand vous ouvrez un fichier Word (.doc), l'antivirus va vérifier qu'il ne contient pas de virus avant de laisser Word accéder au fichier.

En cas de problème, l'antivirus vous préviendra qu'il a trouvé un virus et vous demandera quoi en faire. On peut généralement : bloquer simplement l'accès, essayer de désinfecter le fichier, effacer le fichier ou le mettre en quarantaine.

Chaque antivirus possède une sorte de dictionnaire des virus, appelé *base de signatures*. C'est la liste des signatures, des empreintes des virus. L'antivirus se sert de cette base pour détecter les virus. Il est important de mettre régulièrement à jour cette base de signature, afin que l'antivirus « apprenne » à reconnaître les nouveaux virus. Cela consiste généralement à télécharger un fichier, et certains antivirus font même cela automatiquement, ce qui est encore plus pratique.

L'antivirus est la ceinture de sécurité de l'ordinateur : Ça ne garantit pas que vous n'aurez pas d'accident, mais ça peut vous sauver la vie lors de certains accidents.

2.3 Firewall : J'ai un firewall installé, correctement configuré et qui est mis à jour quand c'est nécessaire

Pourquoi ?

Quand un ordinateur est relié à internet (ou à tout autre réseau), il communique avec d'autres ordinateurs pour échanger des informations. Les programmes qui fonctionnent sur votre ordinateur (navigateur, logiciel de mail et autres) reçoivent et envoient des informations et des ordres (fais ceci, fais cela, donne-moi ceci ...). C'est le fonctionnement normal de tout ordinateur en réseau.

Le tout, c'est de s'assurer que les logiciels ne vont envoyer des informations sans votre accord et que n'importe qui ne va pas demander à vos logiciels de faire n'importe quoi.

C'est à ça que sert le firewall : contrôler quels logiciels vont sur internet et pour y faire quoi, ainsi que contrôler *qui* (et *si* quelqu'un peut se connecter à votre ordinateur, à vos logiciels (et lesquels).

Comment ?

Le firewall est un petit programme qui va intercepter toutes les communications internet et autoriser/interdire chacune de ces communications en fonction d'un nombre de règles que vous aurez vous-même déterminées.

Il va contrôler ce qui *sort* de votre ordinateur, et ce qui y *entre*.

Contrôle de qui sort : Vous aurez par exemple indiqué à votre firewall quels logiciels ont le droit d'aller sur Internet : votre navigateur, votre logiciel de mail... mais pas le traitement de texte ou le logiciel de dessin ! Ils n'ont rien à faire sur Internet.

Il est techniquement possible de mettre un cheval de Troie dans n'importe quel logiciel (jeu, logiciel de dessin, etc.). Le logiciel se lancera normalement, mais le cheval de Troie s'installera en mémoire, masqué, prêt à envoyer des informations vous appartenant sur internet. Vous risquez alors de voir soudainement le programme de dessin vouloir aller sur internet. C'est louche! Ce n'est pas normal. Le firewall vous permettra de voir cela et de le bloquer.

Contrôle de ce qui *entre* : Votre ordinateur peut fournir un tas de services, comme le partage de dossiers Windows. Il est important d'empêcher n'importe qui sur internet d'accéder à ces services. Le firewall va intercepter les tentatives de connexion à votre ordinateur et les bloquer.

Le firewall vous permet d'avoir un meilleur contrôle sur tout ce qui entre et sort de votre ordinateur, permettant ainsi de bloquer pirates, chevaux de Troie et même certains virus. Bien sûr un firewall n'est pas une arme absolue, mais il bloquera la très grande majorité des pirates.

2.3.1 Configurer son firewall

Il est important de bien comprendre comment fonctionne le firewall et de savoir le configurer : le meilleur des firewalls sera inutile s'il est mal configuré ou mal utilisé. Tout comme il est inutile d'avoir des fenêtres double-vitrage blindées si vous laissez la porte d'entrée ouverte.

2.3.2 Mettre à jour son firewall

Parfois, des failles sont découvertes dans les firewalls eux-mêmes! Il est important de mettre de vérifier de temps en temps si une nouvelle version du firewall est disponible. Certains firewall ont une option de mise à jour automatique. Profitez-en.

2.4 Antispyware : J'ai un antispyware que je lance régulièrement et qui est mis à jour régulièrement

Pourquoi ?

Certains logiciels, sous couvert d'être gratuits, contiennent un petit bout de programme qui va espionner ce que vous faites et l'envoyer à une entreprise sur internet qui revendra ces informations marketing. Même les plus grands éditeurs utilisent ce genre de saleté. Par exemple, Windows Media Player 9 informait Microsoft du titre du DVD que vous étiez en train de lire. Ou encore certains logiciels notent la liste de tous les sites que vous avez visité, ou examinent les logiciels que vous avez installé sur votre ordinateur.

Ces logiciels-espions (appelé spywares) sont de plus en plus courant, généralement masqués au sein d'un logiciel, et portent atteinte à votre vie privée.

Comment ?

Il existe des logiciels qui peuvent détecter et éliminer ces saleté : les antispywares.

Pourquoi les antivirus ne les détectent pas ?

Techniquement, ce ne sont pas des virus puisqu'ils ne se reproduisent pas. Il est donc nécessaire d'installer un programme qui détecte spécifiquement les spywares.

3 Pour aller plus loin... et être plus en sécurité

Voici une checklist qui peut vous aider à améliorer la sécurité de votre ordinateur. Ce sont des règles d'«hygiène informatique» à suivre (aussi appelé «safe-hex», par référence au «safe-sex»). Vous n'êtes pas obligé(e) de toutes les respecter et il est possible que certaines règles ne s'appliquent pas à vous. Mais plus vous en appliquerez, plus vous serez en sécurité.

Vous n'êtes pas en mesure de cocher une case? Vous ne comprenez pas? Vous voulez en savoir plus? Pas de panique! Consultez les liens que je vous donne à la fin de ce document (Merci de ne pas me poser de questions par mail).

3.1 Checklist

- J'ai compris qu'un ordinateur, c'est pas un réfrigérateur : c'est beaucoup plus compliqué.
- Je comprend que sans antivirus et sans firewall, je peux être infecté par un virus ou un cheval de Troie depuis des années sans m'en être aperçu.
- J'ai conscience que ne pas protéger mon ordinateur, c'est encourir des risques inutiles et contribuer au bordel ambiant.
- J'ai compris que je suis vulnérable même avec un modem 56K.
- Sur un nouvel ordinateur (ou un ordinateur sur lequel je viens de ré-installer Windows), j'installe un firewall avant ma première connexion à internet.
- J'ai compris qu'il n'existe aucun logiciel (antivirus, firewall ou autre) qui assure une sécurité à 100 %, mais que ces logiciels restent nécessaires.
- J'ai compris que j'ai les moyens de me protéger gratuitement, et que la seule chose que ça me coûtera, c'est du temps et de réflexion.
- J'ai compris que les logiciels, c'est comme le sexe : c'est pas parce que c'est payant que c'est meilleur.
- Je sais utiliser mon antivirus et le configurer. J'en ai lu la documentation.
- J'ai compris que je suis responsable aux yeux de la loi de ce qui est fait avec ma connexion internet.
- J'ai compris que je ne suis pas anonyme sur internet : mon fournisseur d'accès sait qui je suis et peut fournir aux autorités mon identité et adresse.
- J'ai compris que je ne suis anonyme sur internet que tant que je ne donne pas d'informations personnelles, sur un site web ou ailleurs.
- J'ai compris que les adresses d'expéditeur d'email peuvent être totalement falsifiées.
- Je n'envoie jamais la moindre information confidentielle (mot de passe, numéro de carte de crédit...) à ma banque, mon fournisseur d'accès ou toute autre entreprise qui me le demande (Microsoft y compris).
- Je n'ouvre jamais les attachements dont je n'attend pas la réception, même s'ils proviennent (ou semblent provenir) de mon FAI, Microsoft, ou même de mes propres amis
- .
- Je sais configurer Internet Explorer et Outlook Express pour désactiver ActiveX et l'active scripting (VBScript, Javascript, WSH...)
- Je ne clic pas bêtement sur tout fichier que je trouve.
- Je ne lance pas les programmes 'marrants', mêmes envoyés par des amis ou des connaissances.
- Un ami qui place un cheval de Troie sur mon ordinateur n'est pas un ami.
- Quand je choisis un logiciel à télécharger, je m'assure d'abord qu'il ne contient pas de

- spyware.
- Quand je télécharge un programme que je veux installer, je le télécharge toujours d'une source sûre, et si possible directement du site de l'auteur.
- Je veille à ce que la fonction de mise à jour automatique de mon antivirus / firewall / antispyware soit activée et qu'elle fonctionne.
- Si la mise à jour automatique de mon antivirus/firewall/antispyware ne fonctionne pas, je sais où aller télécharger la mise à jour et comment l'installer manuellement.
- Je sais quels programmes sont lancés au démarrage de mon ordinateur et je n'ai laissé que ceux dont j'ai absolument besoin.
- J'ai désactivé tous les services dont je n'ai pas besoin (Windows NT/2000/XP/2003 uniquement).
- J'ai désactivé le partage de fichiers Windows.
- Si j'utilise le partage de fichiers, je ne partage jamais de dossier sans mot de passe.
- J'ai désactivé l'utilisateur invité (guest). (Windows NT/2000/XP/2003 uniquement).
- J'ai désactivé le partage par défaut des disques. (Windows NT/2000/XP/2003 uniquement).
- Je ne travaille pas en tant qu'administrateur (Windows NT/2000/XP/2003 uniquement).
- Je choisis de bons mots de passe.
- Si j'ai des serveurs installés sur mon ordinateur (serveur web (HTTP), FTP, ssh...), je sais les configurer et je les ai correctement configurés.
- Si j'ai des serveurs installés sur mon ordinateur, je les met à jour régulièrement.
- Je n'utilise pas des logiciels en version beta. Je n'utilise que les versions stables.
- Je surveille l'actualité informatique et je réagis en conséquence (patches, mises à jour des logiciels, etc...)
- Je ne désactive jamais mon antivirus, même quand j'insère le CD, la disquette ou la clé USB d'un ami qui m'assure qu'il ne peut y avoir de virus dessus.
- Je sais ce que sont les hoax et je ne me fais pas avoir.
- Je sais ce que sont les scam et je ne me fais pas avoir.
- Je sais ce que sont les spams et je ne me fais pas avoir.
- Je sais interpréter les alertes de mon firewall.
 - J'ai compris quand un programme est censé aller sur internet ou non.
 - J'ai compris ce que sont les tentatives de connexion à mon ordinateur venant d'internet.
 - J'ai compris ce qu'était le mode apprentissage de mon firewall et je sais le désactiver.
- En cas de doute, je sais comment neutraliser ma connexion internet (avec le firewall ou sans).
- Je ferme toujours ma connexion à internet quand je n'en ai pas besoin
- Dans Internet Explorer, je ne clic jamais bêtement 'oui' sur toutes les fenêtres de confirmation qui s'affichent.
- J'ai toujours sous la main l'adresse un forum où je sais que je peux aller demander de l'aide ou des renseignements.
- J'ai toujours sous la main les coordonnées d'un ami «qui s'y connaît en informatique» et qui peut me dépanner en cas de problème.
- J'ai conscience que l'intelligence collective d'un forum est meilleure conseillère que l'«ami qui s'y connaît en informatique».
- J'ai toujours sous la main les URL des antivirus en ligne. On ne sait jamais, ça peut servir.
- Je sais désactiver la restauration système en cas de problème.
- J'ai configuré l'explorateur de Windows pour afficher les extensions de fichiers et fi-

- chiers/répertoires cachés.
- J'ai toujours à portée de main le CD d'installation de Windows, le numéro de série, les pilotes de chacun de mes périphériques (y compris du modem internet), le CD d'installation de mon fournisseur d'accès et les codes d'accès.
 - J'ai au moins une disquette qui me permet de démarrer mon ordinateur dessus et accéder au lecteur de CD-Rom. J'ai vérifié que cette disquette fonctionne bien et que je peux accéder au lecteur de CD-Rom.
 - J'ai une connexion internet de secours (vieux modem téléphonique, autre ordinateur, ami, voisin).
 - Je n'achète jamais ce qu'on me propose par email. Jamais. Jamais jamais. Je boycotte les entreprises qui m'envoie de la publicité non sollicitée.
 - Je ne répond jamais au spam. Je n'essaie pas de me désinscrire.
 - Quand je dois entrer des informations confidentielles (ex : numéro de carte de crédit), je le fais uniquement dans des pages sécurisés (HTTPS), et pas sur un obscure site web.
 - Quand un site me demande mon adresse email, j'évite de la donner, surtout s'ils me promettent des choses gratuitement.
 - J'utilise Spamgourmet.com pour recevoir des mails des sites qui me demandent mon adresse email.
 - J'ai compris que le P2P (Peer-to-peer) est légal, mais que la majorité des fichiers qu'on y trouve sont illégaux.
 - J'ai compris que le P2P est un nid à virus et qu'il est dangereux de télécharger des programmes venant de là.
 - J'ai compris que le MP3 et le DivX sont légaux, mais que que partager ma collection de CD ou toute autre oeuvre protégée par droits d'auteur est illégale, que ça soit par P2P ou tout autre moyen (HTTP, FTP...)
 - J'ai compris qu'utiliser des logiciels piratés, crackés, déprotégés est non seulement illégal, mais aussi dangereux.
 - Je fais régulièrement des copies de sauvegarde de mes fichiers (sur CDR, sur un autre ordinateur, un autre disque dur, sur disquettes, sur clé USB...)
 - Je vérifie que je peux relire mes copies de sauvegarde.
 - Si j'ai une « box »(Freebox, LiveBox, C-Box, AOLBox...) et que l'option « Routeur » est disponible, je l'ai activée.
 - Si j'ai un routeur, j'ai changé le mot de passe par défaut du routeur.
 - Si j'ai une connexion WiFi (ondes radio), j'ai activé la sécurité.

3.2 Notes

1. La sécurité à 100% n'existe pas . Je ne vous garantit rien mais ces règles devraient bien vous aider.
2. J'ai parfaitement conscience que cette liste n'est pas complète. N'hésitez pas à suggérer des améliorations.

3.3 Les explications en détail

3.3.1 J'ai compris qu'un ordinateur, c'est pas un réfrigérateur : c'est beaucoup plus compliqué

Contrairement à ce que voudraient nous faire croire les supermarchés, un ordinateur c'est compliqué. Très compliqué, même. C'est normal.

L'ordinateur va donc exiger de vous de la patience et un minimum de réflexion.

N'oubliez pas qu'un ordinateur, c'est idiot, c'est stupide, c'est bête à manger du foin.

3.3.2 Je comprend que sans antivirus et sans firewall, je peux être infecté par un virus ou un cheval de Troie depuis des années sans m'en être aperçu

La majorité des chevaux de Troie sont totalement invisibles : En effet ils n'affichent rien à l'écran pendant leur fonctionnement, ils ne sont pas visible dans la barre des tâches, et certains n'apparaissent même pas dans la liste des processus en cours.

Un pirate peut donc se servir de votre ordinateur pendant que vous l'utilisez sans que vous vous rendiez compte (Il peut voir ce que vous voyez à l'écran, savoir tout ce que vous tapez au clavier... et même vous voir si vous avez une webcam!).

De même, vous pouvez être infecté par un virus sans le savoir. Certains virus n'annoncent pas leur arrivée et peuvent rester en « sommeil » pendant un certain temps. Sans antivirus, vous pouvez traîner un virus depuis des mois, voir des années sans le savoir. Pendant ce temps, vous infectez des centaines de personnes. Et le jour où il se déclenchera, vous risquez de perdre vos fichiers.

Installez antivirus et antispyware : ils sauront détecter la majorité de ces saletés.

3.3.3 J'ai conscience que ne pas protéger mon ordinateur, c'est encourir des risques inutiles et contribuer au bordel ambiant

Avec un ordinateur non protégé, vous encourez des risques légaux si votre connexion internet est utilisée pour faire des choses illégales. Et vous emmerdez copieusement le reste de la planète en diffusant des virus, du spam et Dieu sait quoi d'autre.

Vous connaissez le spam ? Ces emails publicitaires non sollicités qui veulent vous vendre plein de trucs bizarres (du Viagra liquide, des permis de conduire, des pillules pour augmenter la taille du sexe, etc...). Il faut savoir que la grande majorité de ces spams sont émis à partir d'ordinateurs d'internautes reliés par ADSL et piratés. Les pirates se font grassement payer par les spammeurs pour utiliser les ordinateurs d'innocents internautes pour envoyer des milliers de mails publicitaires. Grâce à cela, les spammeurs peuvent continuer à pourrir la planète en toute impunité, puisqu'on ne peut pas tracer la source des spam.

Ne leur facilitez pas la tâche : protégez votre ordinateur.

Certains fournisseurs d'accès ont également commencé à prendre l'initiative de couper la connexion des internautes qui servent de relai au spam.

Pour vous protéger : Notre carré magique (WindowsUpdate + Antivirus + Firewall + Antispyware) devrait bloquer 99,99% des tentatives de piratage.

3.3.4 J'ai compris que je suis vulnérable même avec un modem 56K

Beaucoup disent qu'avec un simple modem téléphonique 56K, il n'est pas nécessaire d'avoir un firewall.

C'est oublier un peu vite qu'il suffit de quelques seconde à un virus comme Blaster pour s'insérer dans l'ordinateur. Et comme ces virus choisissent au hasard l'adresse IP de la machine cible, ça peut tomber sur vous.

Donc, oui : même avec un simple modem 56K, ces protections sont nécessaires.

3.3.5 Sur un nouvel ordinateur (ou un ordinateur sur lequel je viens de ré-installer Windows), j'installe un firewall avant ma première connexion à internet.

Des virus se baladent sur internet en permanence, à la recherche d'ordinateurs à infecter. L'installation standard de Windows est vulnérable à ces virus, ce qui veut dire que sans firewall l'ordinateur sera infecté *dès les premières minutes de connexion à internet* (Même si c'est un ordinateur que vous venez d'acheter.).

Il vous suffit d'installer un firewall (comme ZoneAlarm). Le firewall bloquera les tentatives d'accès malveillantes pendant que vous faites un WindowsUpdate pour installer toutes les mises à jour critiques.

Pensez à avoir un firewall sur disquettes, clé USB ou CD-Rom. Si c'est votre premier ordinateur, demandez à un ami de vous donner une copie d'un firewall pour que vous puissiez l'installer avant de vous connecter.

L'installation du firewall doit être votre première étape après l'installation de Windows.

3.3.6 J'ai compris qu'il n'existe aucun logiciel (antivirus, firewall ou autre) qui assure une sécurité à 100%, mais que ces logiciels restent nécessaires

Certains disent que les antivirus et firewalls sont inutiles, puisqu'ils ne sont pas fiables à 100%.

C'est abuser !

La ceinture de sécurité ne vous évitera pas les accidents. Il y a même des personnes qui l'avaient mise et sont mortes malgré tout. Mais de là à dire que la ceinture de sécurité est inutile, il y a un gouffre. Dans la grande majorité des cas, ça sauve des vies !

C'est la même chose pour les antivirus.

J'entend déjà certains dire « Si ! L'antivirus ViGuard arrête 100% des virus, parcequ'il n'a pas de système de signatures ! »

Ma réponse :

1. pour le principe : un logiciel fiable à 100%, ça n'existe pas .
2. ViGuard est intéressant, mais il exige de l'utilisateur des connaissances techniques hors de portée de la majorité des utilisateurs.
3. ViGuard n'est pas infaillible : cherchez sur Google, vous verrez qu'il existe divers moyen de le duper et d'infecter un système.
4. ViGuard n'a pas besoin de mise à jour des signatures, mais d'une mise à jour du programme entier. C'est pas mieux.

3.3.7 J'ai compris que j'ai les moyens de me protéger gratuitement, et que la seule chose que ça me coûtera, c'est du temps et de réflexion

Aucune excuse pour ne pas vous protéger : On trouve divers antivirus, firewalls et antispy-wares gratuits et d'excellente qualité !

Sécuriser votre ordinateur vous demandera un peu de temps, de réflexion, peut-être aussi d'énerverment, mais n'hésitez pas à demander de l'aide sur internet : vous trouverez toujours quelqu'un pour vous aider.

Et l'enjeu en vaut la chandelle.

Internet peut être vu comme une grande communauté : en y entrant, c'est quand même la moindre des choses de ne pas pourrir les autres avec des virus et autres saletés, non ? Question de respect.

3.3.8 J'ai compris que les logiciels, c'est comme le sexe : c'est pas parce que c'est payant que c'est meilleur

Certains ne se sentent pas en sécurité avec des antivirus ou firewall gratuits. Ils pensent qu'ils sont moins efficaces. C'est une erreur. Ces produits sont aussi bons, voir meilleurs que les équivalents payants.

En fait ces logiciels gratuits (antivirus ou firewall) sont bien des logiciels commerciaux, faits par des entreprises très sérieuses. Ces entreprises, pour augmenter leur popularité, on décidé d'en faire profiter gratuitement les particuliers. Cela permet d'habituer les gens à utiliser leurs produits et d'assoier leur réputation.

Ces entreprises gagnent de l'argent en vendant leurs logiciels aux entreprises, qui sont de plus gros acheteurs que les particuliers. Seuls les particuliers ont droit aux versions gratuites.

Si vous pensez encore de Norton ou McAfee sont les meilleurs, il serait temps de réviser votre jugement. Ils ont la plus grosse renommée, mais ce ne sont pas les meilleurs.

Je vous encourage à essayer Avast! Home Edition, AntiVir, F-Prot, ZoneAlarm... ce sont d'excellents produits.

3.3.9 Je sais utiliser mon antivirus et le configurer. J'en ai lu la documentation

Avoir une voiture, ça n'est intéressant que si on sait conduire. C'est la même chose avec l'antivirus : apprenez à vous en servir, pour scanner un fichier ou un dossier.

Lisez la documentation de votre antivirus : vous y trouverez tout ce qu'il faut pour bien utiliser votre antivirus, et probablement aussi des conseils.

3.3.10 J'ai compris que je suis responsable aux yeux de la loi de ce qui est fait avec ma connexion internet

C'est un fait : au yeux de la loi, vous êtes responsable de tout ce qui est fait à travers votre connexion internet.

Ne pas protéger votre ordinateur, c'est risquer d'être tenu pour responsable de délits que vous n'avez pas commis vous-mêmes. Et peu importe que vous ne soyez pas coupable : vous aurez beaucoup de mal à le prouver. Aux yeux de votre fournisseur d'accès et de la loi : c'est vous le responsable.

D'ailleurs, relisez attentivement le contrat avec votre fournisseur d'accès : vous verrez qu'il est clairement stipulé que vous êtes seul responsable de la sécurisation de votre ordinateur.

3.3.11 J'ai compris que je ne suis pas anonyme sur internet : mon fournisseur d'accès sait qui je suis et peut fournir aux autorités mon identité et adresse

Vis à vis de votre fournisseur d'accès internet, vous n'êtes pas anonyme. Il sait qui vous êtes et a la possibilité de savoir tout ce que vous faites sur internet. C'est une histoire de confiance. En France, les fournisseurs d'accès ont même l'obligation légale de conserver toutes vos informations de connexion pendant un an.

Seul votre fournisseur d'accès peut savoir que c'est vous qui utilisiez votre adresse IP à un instant donné.

Les fournisseurs d'accès peuvent être forcés par un juge de remettre aux autorités toutes les informations vous concernant.

3.3.12 J'ai compris que je ne suis anonyme sur internet que tant que je ne donne pas d'informations personnelles, sur un site web ou ailleurs

Sur Internet, l'anonymat n'existe pas. Seulement le pseudonymat. (Vous pouvez vous masquer derrière un pseudo, tel que «totor54», et seul votre fournisseur d'accès peut livrer votre réelle identité).

Mais bien sûr, à partir du moment où vous donnez des informations personnelles sur un site, vous n'êtes plus anonyme vis-à-vis de ce site. Et allez savoir ce que ce site va faire de ces informations... De plus, les moteurs de recherche permettent parfois d'aller à la pêche de ces informations, puisque que Google (et autres) parcourent ces sites.

En France, tout fichier nominatif doit être déclaré à la CNIL, mais à l'étranger ce n'est pas la même chose. N'importe qui peut monter un site en Français en Russie ou au Chili et amasser ces informations hors de votre portée et hors de portée de la CNIL.

Soyez donc attentif et ne donnez pas des informations personnelles au premier venu.

3.3.13 J'ai compris que les adresses d'expéditeur d'email peuvent être totalement falsifiées

N'ayez aucune confiance dans l'adresse des expéditeurs de mail. Ça peut se falsifier facilement. N'importe qui est capable d'envoyer des mails en se faisant passer pour Microsoft ou l'abbé Pierre.

C'est facile : il suffit d'aller dans la configuration de votre logiciel d'email et d'entrer l'adresse de l'expéditeur de votre choix (Bill.Gates@Microsoft.com, etc.)

Par conséquent, n'importe qui peut usurper l'identité de vos amis, ou de vous même ! Les virus font également très souvent ce genre de chose.

Soyez donc méfiant.

Note : si vous voulez être sûr de l'identité de l'expéditeur d'un mail, il faut que vous et votre correspondant utilisiez des logiciels comme PGP ou GPG (voir <http://sebsauvage.net/logiciels/pgp.html>)

3.3.14 Je n'envoie jamais la moindre information confidentielle (mot de passe, numéro de carte de crédit...) à ma banque, mon fournisseur d'accès ou toute autre entreprise qui me le demande (Microsoft y compris)

Les entreprises (banques, sites web et autres) ne demandent *jamais* ces informations par email. Il n'y a aucune raison de leur envoyer. C'est probablement une usurpation d'identité : le mail n'a pas été écrit par qui il prétend l'être.

Si quelqu'un vous demande votre mot de passe ou toute autre information confidentielle, c'est très probablement pour tenter de vous arnaquer, de vous voler votre mot de passe.

Les banques ne demandent jamais des numéros de carte de crédit par email. Cela passe toujours par des pages sécurisées directement sur le site de la banque.

Votre fournisseur d'accès ne vous redemande jamais votre mot de passe. Il n'en a pas besoin, puisqu'il peut le changer comme il veut.

C'est la même chose pour le reste (mail, boutiques en ligne, etc.)

Ne vous faites pas avoir.

3.3.15 Je n'ouvre jamais les attachements dont je n'attend pas la réception, même s'ils proviennent de mon FAI, Microsoft, ou même *de mes propres amis*

Votre Fournisseur d'Accès à Internet (FAI), Microsoft ou les éditeurs d'antivirus n'envoient jamais des fichiers, programmes, patches, correctifs ou antivirus par email. Il faut toujours les télécharger directement sur leur site.

De même, soyez méfiant quand vous recevez d'un inconnu une soit-disant image, jeu ou économiseur d'écran : Il est très probable que ça soit un virus ou un cheval de Troie.

Et même si ce fichier vient de vos amis ! Pourquoi se méfier de vos amis ? Parcequ'ils peuvent être infecté par un virus qui a envoyé un mail infecté à leur insu, en leur nom.

Par précaution, n'ouvrez pas un attachement si ça n'est pas quelque chose que vous attendiez à recevoir.

3.3.16 Je sais configurer Internet Explorer et Outlook Express pour désactiver ActiveX et l'active scripting (VBScript, Javascript, WSH...)

Microsoft a inclus plein de fonctionnalités dans ses logiciels, y compris l'active scripting (qui permet d'inclure dans les documents de petits programmes qui s'exécutent automatiquement et font plein de choses) et l'ActiveX (qui permet d'inclure des programmes dans les pages web qui se téléchargent et s'exécutent automatiquement).

C'est très sympa, mais c'est aussi dangereux. Cela permet à n'importe qui de créer un programme qui va automatiquement s'exécuter sur votre ordinateur, et de mettre ce programme dans une page web ou dans un simple email.

Il est important de désactiver ces systèmes dans Internet Explorer et Outlook Express (sauf sur certains sites de confiance). Allez dans la configuration de ces logiciels et désactivez-les.

N'oubliez pas qu'il existe d'autres navigateurs (comme Mozilla Firefox) ou logiciels d'email (comme Thunderbird) qui n'ont pas ce genre de problème. Ce sont d'excellents logiciels qui peuvent les remplacer avantageusement. Non seulement ils sont plus sûrs, mais ils sont plus agréables à utiliser :

- <http://sebsauvage.net/logiciels/firefox.html>
- <http://sebsauvage.net/logiciels/thunderbird.html>

3.3.17 Je ne clique pas bêtement sur tout fichier que je trouve

La curiosité est loin d'être un défaut en informatique, mais soyez quand même prudent !

Double-cliquer sur un fichier ça veut dire « ouvrir le fichier » ou « lancer le programme ». Et ce programme pourrait très bien être un virus. Et certains programmes (virus) sont même capable de se déguiser en simple fichier.

3.3.18 Je ne lance pas les programmes 'marrants', mêmes envoyés par des amis ou des connaissances

Ça peut effectivement être un simple programme marrant, mais il y a aussi de fortes chances que ça soit un virus ou un cheval de Troie. Autant ne pas prendre de risques inutiles.

3.3.19 Un ami qui place un cheval de Troie sur mon ordinateur n'est pas un ami

Que diriez-vous d'un ami qui a forcé votre porte d'entrée «pour rigoler»? Et qui a installé micros et caméras chez vous «pour rigoler»? C'est la même chose avec un cheval de Troie dans votre ordinateur. Moi, je n'appelle pas ça un ami.

Et même si il n'a pas de mauvaises intentions, le cheval de Troie peut ouvrir l'accès à votre ordinateur à la planète entière. Pour dire les choses crûment : Vous êtes à poil sur internet.

Comme on dit, avec des amis comme ça, on a pas besoin d'ennemis.

3.3.20 Quand je choisis un logiciel à télécharger, je m'assure d'abord qu'il ne contient pas de spyware

Un certains nombre de logiciels contiennent des spywares. Ces programmes vont espionner ce que vous faites. Ça peut aller de la liste des sites que vous visitez, la liste des fichiers téléchargés jusqu'à la liste complète des logiciels que vous avez installé sur votre ordinateur.

Je ne sais pas pour vous, mais personnellement, j'ai horreur qu'on pose des caméras chez moi pour m'espionner. Evitez donc ces programmes. Par exemple GetRight et ReGet sont des logiciels d'aide au téléchargement. Ils contiennent des spywares. Laissez-les tomber! Et prenez des logiciels équivalents sans spyware comme Free Download Manager .

Vérifiez si ces logiciels contiennent un spyware avant de les télécharger. Voici quelques sites qui pourront vous donner des informations :

- <http://www.spychecker.com>
- <http://www.spywareinfo.com>
- <http://www.safer-networking.org>
- <http://www.spywareguide.com>
- <http://grc.com/oo/suspects.htm>

Et même après avoir installé un logiciel, passez un petit coup d'antispyware pour vous en assurer.

3.3.21 Quand je télécharge un programme que je veux installer, je le télécharge toujours d'une source sûre, et si possible directement du site de l'auteur

Ne téléchargez pas vos logiciels n'importe où.

N'allez pas télécharger un programme sur le site d'un obscure inconnu. Cet inconnu a très bien pu greffer un cheval de Troie sur le programme. Ou même s'il n'a pas de mauvaises intentions, son ordinateur a peut-être été infecté par un virus.

De préférence, allez télécharger les programmes directement sur le site de l'auteur. Par exemple, téléchargez Mozilla uniquement sur le site mozilla.org. Et ainsi de suite pour les autres programmes.

Certains sites spécialisés en téléchargement sont également une source fiable, car ils font attention. Par exemple : Nonags.com, Snapfiles.com, Telechargez.com, Clubic.com, CNet.com, Download.com, ZDNet.fr; etc. On peut considérer ces sites comme sûrs (et encore...)

3.3.22 Je veille à ce que la fonction de mise à jour automatique de mon antivirus/firewall/antispyware soit activée et qu'elle fonctionne

Si votre antivirus n'est pas à jour, il ne détectera pas les derniers virus, et les laissera tranquillement infecter votre ordinateur. C'est la même chose avec l'antispyware : il doit être mis à jour de temps en temps pour détecter les nouvelles saletés.

De temps en temps, on découvre des failles dans les firewalls. Ces failles pourraient permettre à un pirate de pénétrer dans votre ordinateur. Il est important de mettre le firewall à jour avant qu'un pirate ait eu le temps d'exploiter cette faille.

Par chance, la plupart des antivirus, antispywares et firewalls ont des fonctions de mise à jour automatique qui iront automatiquement vérifier si des mises à jour sont disponibles.

Mais il ne suffit pas d'activer la mise à jour automatique : vérifiez qu'elle fonctionne bien. Ça serait dommage de laisser tourner votre antivirus sans surveillance pour vous apercevoir que cela fait plusieurs mois qu'il n'arrive pas à se mettre à jour.

3.3.23 Si la mise à jour automatique de mon antivirus / firewall / antispyware ne fonctionne pas, je sais où aller télécharger la mise à jour et comment l'installer manuellement

Il arrive que la mise à jour automatique ne fonctionne pas, ou que le programme n'en soit pas équipé. Dans ce cas, il est important de savoir faire cette mise à jour manuellement.

Par exemple la plupart des éditeurs d'antivirus vous proposent de télécharger un fichier (un programme ou un simple fichier) à exécuter ou à placer à un endroit précis pour mettre à jour votre antivirus. Malheureusement, il est parfois difficile de trouver ces fichiers sur leur site web.

Voici quelques adresses (il est possible que ces adresses aient déjà changé depuis que je les ai écrites) :

- **AntiVir Personal Edition :**
<http://www.free-av.de/down/vdf/vdfh.zip> ou
<http://www.free-av.com/down/vdf/vdfh.zip> Dézippez le fichier dans le répertoire où AntiVir est installé.
- **Tous les antivirus McAfee/Network Associates :**
http://www.mcafeesecurity.com/us/downloads/updates/superdat_download.asp
Téléchargez sdatXXXX.exe et exécutez ce programme.
- **F-Prot : Téléchargez les 2 fichiers suivants :**
http://www.f-prot.com/cgi-bin/get_randomly?fp-def
http://www.f-prot.com/cgi-bin/get_randomly?macrdef2
et dézippez le contenu de ces 2 fichiers ZIP dans le répertoire de F-Prot (en écrasant les fichiers déjà présents).
- **AVG Free Edition :** http://www.grisoft.com/us/us_updt6.php?lng=fe
Téléchargez le fichier .bin, placez-le dans le répertoire UPDATE d'AVG et lancez AVG.
- **Avast ! 4.1 Home Edition :** <http://www.avast.com/iavs4pro/vpsupd.exe>
Exécutez ce programme.

3.3.24 Je sais quels programmes sont lancés au démarrage de mon ordinateur et je n'ai laissé que ceux dont j'ai absolument besoin

Beaucoup de chevaux de Troie et spyware vont s'incruster dans Windows et démarrer automatiquement en même temps que Windows. Il peut être intéressant de jeter un coup d'oeil de

temps en temps pour voir qui s'est installé là.

De plus, plus vous avez de programmes en mémoire, plus le risque est grand qu'un pirate profite des bugs d'un de ces programmes pour pénétrer dans votre ordinateur. Comme certains de ces programmes ouvrent des ports en écoute (sur votre connexion internet), arrêter ces programmes fermera les ports correspondants.

Moins de programmes en mémoire, c'est moins de risque, mais c'est aussi une machine plus agréable à utiliser puisqu'elle démarre plus vite et qu'il y a plus de mémoire libre. Des programmes comme AutoStart Manager

<http://sebsauvage.net/logiciels/autostartmanager.html> peuvent vous aider à voir quels sont les programmes lancés au démarrage et les désactiver.

3.3.25 J'ai désactivé tous les services dont je n'ai pas besoin (Windows NT / 2000 / XP / 2003 uniquement)

En plus des programmes lancés au démarrage, ces versions de Windows ont également un système de *services*.

Ces services sont des programmes qui sont lancés automatiquement au démarrage de Windows afin de fournir... des services (par exemple, le parcours du réseau local, le partage de fichiers, l'accès distant à la base de registre, serveur web...).

Chaque service lancé, c'est un risque supplémentaire. Un service bugué ou mal configuré pourrait permettre à un pirate de pénétrer dans l'ordinateur.

Principe de précaution : désactivez tous les services dont vous n'avez pas besoin (C'est dans le panneau de configuration).

Le fait d'arrêter ces services fermera les ports correspondants.

3.3.26 J'ai désactivé le partage de fichiers Windows

Le partage de fichiers Windows est très pratique pour échanger des fichiers d'un ordinateur à l'autre. Malheureusement, il est aussi très pratique pour s'introduire dans un ordinateur. Et comme il est activé par défaut, c'est un danger.

Il faut aller dans le panneau de configuration, partie réseau, et soit supprimer ce service (si vous n'en avez pas besoin) ou au moins le configurer pour qu'il ne serve pas des fichiers sur l'interface (modem, carte réseau...) reliée à internet.

3.3.27 Si j'utilise le partage de fichiers, je ne partage jamais de dossier sans mot de passe

Si vous utilisez le partage de fichier, mettez au moins un mot de passe sur le chaque dossier partagé.

Chez vous, vous n'avez peut-être pas de porte blindée, mais vous utilisez au moins une serrure.

C'est la même chose pour le partage de fichiers : ne leur facilitez pas la tâche en laissant tout grand ouvert.

Note : les partages cachés (ceux dont le nom se termine par \$) *ne sont pas cachés*. Il y a des astuces qui permettent de les voir malgré tout.

3.3.28 J'ai désactivé l'utilisateur invité (guest). (Windows NT / 2000 / XP / 2003 uniquement)

L'utilisateur invité (guest) est un utilisateur automatiquement créé lorsque vous installez Windows. D'habitude, on ne s'en sert jamais et on a vite fait de l'oublier : Mais il est là, et il a le droit de faire des choses dans l'ordinateur.

Autant le désactiver pour que personne ne s'en serve.

3.3.29 J'ai désactivé le partage par défaut des disques. (Windows NT / 2000/ XP / 2003 uniquement)

Quand vous installez Windows, Windows décide de lui-même d'utiliser le partage de fichiers pour partager les disques C :, D :, etc. (Il sont partagé en tant que C\$, D\$, etc.). C'est très pratique pour l'administration en entreprise, mais cela permet aussi potentiellement à n'importe qui d'accéder au contenu complet de votre disque dur !

Autant ne pas prendre de risque et désactiver cela.

3.3.30 Je ne travaille pas en tant qu'administrateur (Windows NT / 2000 / XP / 2003 uniquement)

L'administrateur peut tout faire sur l'ordinateur, y compris aller bidouiller le système d'exploitation et modifier des fichiers système.

Si vous travaillez en administrateur et que par inadvertance vous lancez un programme malveillant, ce programme pourra aller modifier ce qu'il veut dans le système. C'est dangereux.

En travaillant avec un simple utilisateur, si vous lancez ce même programme malveillant, il ne pourra pas aller modifier les fichiers système et aura plus de mal à s'installer dans votre ordinateur.

3.3.31 Je choisis de bons mots de passe

Si quelqu'un trouve votre mot de passe, il pourra accéder à votre ordinateur et faire ce qu'il veut, même à distance par internet.

Il est donc important de choisir de bons mots de passe.

- Ils ne doivent pas être trop courts.
- Ils ne doivent pas être des mots du dictionnaire ou des noms propre (prénoms, noms de famille, noms de villes, etc.).
- Ils ne doivent pas être des dates d'anniversaire.
- Ils ne doivent pas être en relation avec vous (le nom de votre ami(e), du chat, du chien, etc.).

Les pirates ont des logiciels qui essaient automatiquement tous les mots du dictionnaire, prénoms, noms et dates avec toutes les variations possibles (robert51, rosiers789, marseille007, etc.).

Idéalement, le mot de passe fait au minimum 8 caractères, et contient lettres, chiffres et symboles (*\$%@#&...) et n'a aucune signification.

Astuce : Mémorisez une phrase, et utilisez la première lettre de chaque mot. Ajoutez ensuite quelques lettres et symboles (au début ou à la fin du mot de passe). Cela permet de créer des mots de passe longs, sans signification et facile à retenir. Exemple : « La mère michèle n'a pas perdu son chat botté »—j lmmnppscb\$77

3.3.32 Si j'ai des serveurs installés sur mon ordinateur (serveur web (HTTP), FTP, ssh...), je sais les configurer et je les ai correctement configurés

Un serveur mal configuré pourrait permettre à un pirate d'accéder à votre ordinateur.

Par exemple, un serveur FTP où vous avez laissé le compte *Anonymous* actif, ou bien un utilisateur dont vous n'avez pas restreint les droits d'accès pourrait aller lire (et éventuellement) modifier n'importe quel fichier sur votre disque dur.

Lisez la documentation de vos serveurs afin de bien les configurer.

3.3.33 Si j'ai des serveurs installés sur mon ordinateur, je les met à jour régulièrement

Des failles sont régulièrement découvertes dans divers serveurs (FTP, HTTP (comme Apache, IIS...)). Tenez-vous au courant mettez promptement à jour vos différents serveurs quand des failles sont découvertes.

C'est la paresse dans l'installation des mises à jour qui a permis à des virus comme SQL Slammer d'infecter des milliers d'ordinateurs.

3.3.34 Je n'utilise pas des logiciels en version beta. Je n'utilise que les versions stables

Les versions beta sont bien sûr plus récentes, avec peut-être plus de nouvelles fonctionnalités, mais peut-être aussi plus de bugs.

Et tout bug est un risque pour la sécurité.

3.3.35 Je surveille l'actualité informatique et je réagis en conséquence (patches, mises à jour des logiciels, etc...)

Comment savoir si des failles ont été découvertes dans les logiciels que vous utilisez sans suivre l'actualité ?

Il existe divers sites qui vous donnent l'actualité en matière de sécurité, comme Secusys.com, CERT.org, SANS.org, etc.

En suivant l'actualité ainsi, vous pourrez prendre les mesures nécessaires au bon moment. Et même si aucun patch n'est disponible pour l'un de vos logiciels, les bulletins d'alerte sur ces sites vous donneront des moyens de combler temporairement la brèche.

3.3.36 Je ne désactive jamais mon antivirus, même quand j'insère le CD, la disquette ou la clé USB d'un ami qui m'assure qu'il ne peut y avoir de virus dessus

Personne n'est parfait. Même si votre ami(e) vous assure qu'il ne peut pas y avoir de virus, qu'est-ce qui vous le prouve ? Est-ce qu'il utilise un antivirus ? Si oui, lequel ? Est-ce qu'il est à jour ?

Bref... ça fait beaucoup d'inconnues. Autant ne pas prendre de risque inutile.

3.3.37 Je sais ce que sont les hoax et je ne me fais pas avoir

Les hoax, ce sont des canulars. Généralement, le mail vous demande d'envoyer ce message au plus grand nombre de personnes possible. C'est un signe caractéristique de ce genre de mail.

Ne propagez jamais ce mail, même si c'est soit-disant un petit cancéreux qui veut récolter de l'argent ou recevoir des messages de sympathie. C'est malheureux d'avoir à dire ça, mais la plupart du temps ce ne sont que ces canulars, ou bien de mauvaises blagues pour engorger l'adresse email de quelqu'un.

Ces messages peuvent contenir à peu près n'importe quel genre d'information bidon : problème de santé publique, rumeurs, alertes de virus, problèmes de sécurité informatique, information provenant du gouvernement, pétitions, etc.

Ayez l'esprit critique, et ne croyez pas aveuglément tout ce qui se dit sur internet. Le site <http://www.hoaxbuster.com> vous tiendra au courant des hoaxs les plus répandus.

3.3.38 Je sais ce que sont les scam et je ne me fais pas avoir

Le plus courant est le scam nigérien : un dignitaire d'un pays d'Afrique vous demande de servir d'intermédiaire pour une transaction financière importante, en vous promettant un bon pourcentage de la somme. Pour amorcer la transaction, il vous faut donner de l'argent.

C'est bien entendu une arnaque !

Certains naïfs se sont fait voler des dizaines de milliers d'euros. Ne répondez pas.

3.3.39 Je sais ce que sont les spams et je ne me fais pas avoir

Le spam, ce sont ces emails publicitaires que vous recevez.

Ce sont des publicités pour vous vendre n'importe quoi : des médicaments, du viagra liquide, des diplômes, des permis de conduire, des passeports, d'autres papier officiels, des crédits, des logiciels, du matériel informatique, des cartouches d'encre, des pilules pour augmenter la taille du pénis, des publicités pour des sites porno ou bien une astuce pour gagner des centaines d'euros en restant chez vous.

La plupart de ces mails sont bien entendu des arnaques.

3.3.40 J'ai compris quand un programme est censé aller sur internet ou non

Il est normal que certains logiciels aillent sur internet (navigateur, logiciel de mail, jeu en réseau, chat, etc.). Pour certains logiciels, ça peut arriver occasionnellement (par exemple, l'antivirus va de temps en temps sur internet pour se mettre à jour). Mais pour certains logiciels, ça n'est pas justifié du tout ! (par exemple un programme de dessin ou un traitement de texte.).

Un programme qui va sur internet alors que vous ne lui avez rien demandé de tel devrait tout de suite attirer votre attention. Posez-vous la question : est-ce que c'est normal ?

Dans le doute, bloquez avec le firewall et regardez si le programme fonctionne correctement. Regardez aussi dans l'aide du logiciel ou dans sa configuration si il ne possède pas une option de mise à jour automatique. Si ce n'est pas le cas, c'est louche !

3.3.41 J'ai compris ce que sont les tentatives de connexion à mon ordinateur venant d'internet

Quand votre firewall affiche une fenêtre pour dire qu'il y a eu une tentative de connexion sur un port, cela veut juste dire ceci :

Un logiciel, quelquepart sur internet, est venu faire « toc toc ! Est-ce qu'il y a un programme en écoute sur ce port ? ». Rien de plus.

Ce n'est pas forcément une attaque. C'est peut-être juste un logiciel qui essaie de communiquer avec vous. Cela arrive souvent, voire très très souvent (plusieurs centaines de fois par jour). C'est le fonctionnement normal de TCP/IP.

Les logiciels qui essaient de communiquer avec le vôtre peuvent être : des logiciels de chat (dialogue en direct), des serveurs de jeu en réseau, des logiciels de Peer-to-peer (P2P, partage de fichier), etc.

Cela peut arriver parfois parce que vous avez récupéré l'adresse IP de quelqu'un qui vient de se déconnecter, ou bien parce qu'un logiciel quelquepart sur internet déconne et se trompe d'adresse IP.

De plus, quand vous voyez une alerte du firewall « Attaque sur le port BackOrifice », ça ne veut pas dire que vous êtes infecté ou attaqué par BackOrifice ! Ça veut juste dire que quelqu'un sur internet vient faire « toc toc ! » pour voir si, par hasard, il n'y aurait pas un serveur en écoute sur ce port (qui est habituellement utilisé par BackOrifice, mais ce n'est pas obligatoire).

Puisque votre firewall a bloqué la tentative de connexion, vous ne craignez rien.

Pour en savoir plus sur la notion de port, voir

<http://sebsauvage.net/comprendre/tcpip/> et

<http://sebsauvage.net/comprendre/firewall/>.

3.3.42 J'ai compris ce qu'était le mode apprentissage de mon firewall et je sais le désactiver

Votre firewall vous affiche des tas de fenêtres d'alerte. Plein plein. C'est pénible, c'est vrai. Mais c'est normal : il est configuré pour faire cela. Ces fenêtres d'alerte sont conçues pour permettre de créer rapidement et facilement la liste de règles de votre firewall. Cela s'appelle généralement « *mode apprentissage* ».

Cela vous permet de définir quels logiciels ont le droit d'aller sur Internet.

Une fois la liste des règles établie, il vous suffit de modifier la configuration de votre firewall pour ne plus afficher ces alertes, et vous pourrez travailler en sérénité.

Il faudra seulement réactiver le mode apprentissage lorsque vous installerez un nouveau logiciel, histoire de créer la règle adaptée à ce logiciel. Vous pouvez également entrer la règle à la main dans votre firewall (si il dispose de cette fonctionnalité).

3.3.43 En cas de doute, je sais comment neutraliser ma connexion internet (avec le firewall ou sans)

Si vous décelez une activité suspecte sur votre connexion internet, il peut être intéressant de neutraliser immédiatement toute communication le temps d'investiguer. La majorité des firewalls personnels possèdent une option « Bloquer tout le trafic ». Cela neutralise toutes les communications entrantes et sortantes.

Un second clic vous permet de réactiver les communications.

Si votre firewall ne possède pas cette fonction, vous pouvez vous déconnecter, ou au pire débrancher la prise du modem !

3.3.44 Je ferme toujours ma connexion à internet quand je n'en ai pas besoin

Un fait tout simple : un ordinateur qui n'est pas relié à internet ne peut pas être attaqué à distance.

C'est tout bête, mais il suffisait d'y penser : Quand vous n'avez pas besoin de votre connexion internet, déconnectez-vous.

Pas la peine d'être relié à internet quand vous tapez un document dans Word ou jouez à un jeu. Pas la peine de continuer à prendre des risques pour rien.

C'est particulièrement vrai pour les personnes qui ont l'ADSL, surtout quand votre ordinateur reste allumé 24h/24.

3.3.45 Dans Internet Explorer, je ne clic jamais bêtement 'oui' sur toutes les fenêtres de confirmation qui s'affichent

Internet Explorer possède un système appelé ActiveX qui permet de télécharger et exécuter automatiquement des programmes dans les pages web. Ça permet de faire plein de choses intéressantes, mais c'est aussi un risque majeur.

La plupart du temps, quand un contrôle ActiveX veut s'exécuter, Internet Explorer vous affiche une fenêtre d'alerte. Ne cliquez pas bêtement « oui » pour autoriser le contrôle ActiveX à s'exécuter : vérifiez si ce contrôle est signé.

S'il est signé par Microsoft ou une autre société connue (VeriSign, Yahoo...), il n'y a a priori pas de risque. Mais soyez vigilant.

3.3.46 J'ai toujours sous la main l'adresse un forum où je sais que je peux aller demander de l'aide ou des renseignements

Il faut bien l'avouer : en informatique comme ailleurs, on ne peut pas tout savoir.

Les forums sont lus par des dizaines, voir des centaines de personnes différentes. Il y a d'excellentes chances que vous y trouviez quelqu'un qui sache répondre à vos questions, vous aider ou au moins vous donner une piste.

Il y a de nombreux forums sur Internet, à commencer par Usenet (les fameux « newsgroups »), mais aussi un tas de forum sur le web : CommentCaMarche, Clubic, Hardware.fr, Assiste.com...

3.3.47 J'ai toujours sous la main les coordonnées d'un ami « qui s'y connaît en informatique » et qui peut me dépanner en cas de problème

Les forums sont une aide formidable, mais quand votre connexion internet ne fonctionne plus, ça ne vous sera pas d'une grande aide.

Avoir un ami ou une connaissance qui s'y connaisse un peu, ça peut dépanner.

3.3.48 J'ai conscience que l'intelligence collective d'un forum est meilleure conseillère que l' « ami qui s'y connaît en informatique »

Comme en médecine, 2 avis valent mieux qu'un. Et 10 avis valent mieux que 2.

L'intelligence collective, et la somme de savoir d'un forum a plus de chance de vous donner la bonne réponse qu'une personne seule. Tant que c'est possible, venez sur le forum.

Et commencez par chercher sur le forum : il est très probable que quelqu'un a déjà eu le même problème que vous, et que tout le monde lui ai déjà donné la solution, peut-être même plusieurs solutions à son problème.

Cela évitera de déranger votre « ami qui s'y connaît en informatique ».

3.3.49 J'ai toujours sous la main les URL des antivirus en ligne. On ne sait jamais, ça peut servir

Si vous avez un doute sur votre antivirus ou un fichier, il peut être intéressant d'avoir un autre avis. Les antivirus en ligne sont capables de scanner votre ordinateur sans avoir à installer quoi que ce soit.

Accessoirement, cela vous permet de débarquer sur n'importe quel ordinateur et de le scanner sans rien installer. Ça peut être pratique pour dépanner quelqu'un, ou bien vérifier un ordinateur avant d'insérer sa clé USB dedans.

Pour cela, il vous suffit de prendre Internet Explorer et d'aller sur l'un des sites suivants :

- <http://webscanner.kaspersky.fr/>
- <http://housecall.trendmicro.com/>
- <http://www.secuser.com/outils/antivirus.htm> (c'est le même que TrendMicro)
- <http://www.bitdefender.com/>
- <http://www.pandasoftware.com/activescan/>
- <http://security.symantec.com/ssc/>
- <http://www.commandondemand.com/eval/cod/>

3.3.50 Je sais désactiver la restauration système en cas de problème

La restauration système est un système qui permet à Windows de s'auto-réparer (dans une certaine mesure).

Le problème, c'est que les virus peuvent dans certains cas infecter la restauration système elle-même.

Du coup, si vous désinfectez un fichier système, Windows va vouloir le « réparer » et va remettre le virus! Un comble.

Dans certains cas il faut donc être capable de désactiver la restauration système afin de pouvoir correctement désinfecter un ordinateur. Vous trouverez des informations sur la restauration système sur de nombreux sites. Il vous suffit de rechercher sur Google.

Mais n'oubliez pas qu'il vaut mieux prévenir que guérir : installez un antivirus pour bloquer le virus avant qu'il infecte votre système.

3.3.51 J'ai configuré l'explorateur de Windows pour afficher les extensions de fichiers et fichiers/répertoires cachés

Par défaut, l'explorateur de Windows n'affiche pas les extensions des fichiers. C'est très gênant.

Par exemple, « **oiseau.jpg** » apparaîtra comme « **oiseau** » à l'écran. Et « **oiseau.exe** » apparaîtra aussi comme « **oiseau** ». Confusion garantie.

Et c'est même pire : **oiseau.jpg.exe** (qui est bien un programme), apparaîtra comme « **oiseau.jpg** », vous faisant croire que c'est une inoffensive image alors que c'est un programme! On a vite fait de double-cliquer dessus. Et si c'est un virus...

Je vous conseille fortement de configurer l'explorateur pour afficher les extensions des fichiers.

3.3.52 J'ai toujours à portée de main le CD d'installation de Windows, le numéro de série, les pilotes de chacun de mes périphériques (y compris du modem internet), le CD d'installation de mon fournisseur d'accès et les codes d'accès

Les virus peuvent endommager les fichiers et les rendre inutilisables. Les chevaux de Troie vont s'incruster dans le système, parfois en modifiant des fichiers système. Avec tout cela, il n'est pas rare que vos logiciels plantent, que Windows ne démarre plus ou que votre connexion internet ne fonctionne plus.

Il est intéressant d'avoir tout le nécessaire sous la main, afin de pouvoir réinstaller ce qui ne fonctionne plus. Ça peut aller d'un simple programme jusqu'au système entier.

Avoir le CD d'installation du fournisseur d'accès et les codes est utile pour accéder à internet afin d'obtenir de l'aide, et les programmes nécessaires pour réparer.

3.3.53 J'ai au moins une disquette qui me permet de démarrer mon ordinateur dessus et accéder au lecteur de CD-Rom. J'ai vérifié que cette disquette fonctionne bien et que je peux accéder au lecteur de CD-Rom

Si votre CD de Windows n'est pas bootable (si vous ne pouvez pas directement démarrer dessus), en cas de problème, vous serez dans l'impossibilité de ré-installer Windows. Dans ce cas, créez une disquette bootable : Certaines versions de Windows possèdent un outil pour créer cette disquette, et on trouve également des disquettes bootables sur internet :

- <http://www.bootdisk.com/>
- <http://www.powerload.fsnet.co.uk/bootdisk.htm>
- <http://www.bootdisk.info/modules.php?name=Downloads>
- <http://terrikaduck.netfirms.com/bootdisks.htm>
- <http://severinterrier.free.fr/Boot/CDBoot.htm>
- <http://severinterrier.free.fr/Boot/PE-Builder/>

Et surtout, assurez-vous que votre disquette fonctionne et que vous arrivez bien à accéder au lecteur de CD-Rom avec cette disquette.

Il arrive souvent que les disquettes aient des secteurs défectueux, et c'est toujours désagréable de s'en apercevoir au moment où vous en avez vraiment besoin.

3.3.54 J'ai une connexion internet de secours (vieux modem téléphonique, autre ordinateur, ami, voisin)

C'est tout bête, mais même à l'époque de l'ADSL, nos bon vieux modems 56K restent beaucoup plus fiables. Si vous avez un problème ADSL, vous serez bloqué et ne pourrez pas télécharger ce qu'il faut, ou demander de l'aide.

A défaut, demandez à votre voisin, ami ou même allez dans un cybercafé ou un magasin d'informatique pour voir s'ils ne pourraient pas télécharger le pilote ou le programme qui pourrait vous dépanner.

3.3.55 Je ne répond jamais au spam. Je n'essaie pas de me désinscrire

Ne répondez jamais à un spam, même pour dire « *Je n'en veux pas, laissez-moi tranquille !* ». En effet, le simple fait de répondre confirme au spammeur que votre adresse email est valide et qu'il y a bien un humain derrière, qui lit ses mails. Votre adresse email prend alors immédiatement de la valeur à leur yeux, et ils peuvent la revendre.

De même, la grande majorité des liens pour se « dé-inscrire » sont des attrape-nigauds qui vont confirmer que votre adresse email est valide. Vous risquez de recevoir encore plus de spam.

3.3.56 Quand je dois entrer des informations confidentielles (ex : numéro de carte de crédit), je le fais uniquement dans des pages sécurisées (HTTPS), et pas sur un obscure site web

Quand vous donnez des informations confidentielles, comme un numéro de carte de crédit, ne le faites que sur des pages sécurisées (HTTPS). Vous verrez généralement un petit cadenas dans un coin de la fenêtre du navigateur qui vous indiquera que la page est sûre.

Quand je dis « sûre », cela veut dire que personne, entre vous et le site web, ne peut « voler » votre numéro de carte de crédit.

Mais même si le site web est en HTTPS, il ne faut pas donner son numéro de carte de crédit à n'importe quel site web.

Si c'est le site d'une banque, c'est a priori sans risque. Si c'est un grand site comme la FNAC, CDiscount ou Amazon, il n'y a a priori pas de risque. Mais évitez les obscures sites web : vous ne savez pas qui est à l'autre bout, ni ce qu'il va faire de votre numéro de carte de crédit. Et même si il n'a aucune mauvaise intention, son serveur web n'est peut-être pas assez protégé et il peut se faire voler ses numéros de carte de crédit, y compris le vôtre. C'est déjà arrivé!

Préférez les commerçants dont les transactions sont faites directement par les banques (c'est à dire que c'est sur le site d'une banque que vous entrez votre numéro de carte de crédit). Ainsi le commerçant n'est jamais en possession de votre numéro de carte.

3.3.57 Quand un site me demande mon adresse email, j'évite de lui donner, surtout si ils me promettent des choses gratuitement

Ne donnez pas votre adresse email au premier venu : vous avez de fortes chances de recevoir du spam par la suite. Surtout si le site annonce en gros « Free!!! Free!!! Gratuit!!! ». Méfiez-vous.

Beaucoup de site demandent votre adresse email sans raison, par exemple rien que pour pouvoir télécharger un fichier ou accéder à une page gratuite.

Pourquoi font-ils cela ? La plupart du temps, pour pouvoir revendre votre adresse email. (On trouve parfois en vente des CD-Roms contenant des centaines de milliers d'adresses email.)

3.3.58 J'utilise Spamgourmet.com pour recevoir des mails des sites qui me demandent mon adresse email

Si vous devez absolument donner votre adresse email pour recevoir un email d'un site web, utilisez Spamgourmet.com (<http://spamgourmet.com>).

Ce service gratuit permet de créer des *adresses emails jetables* pour recevoir des emails (et aussi pour en envoyer).

Spamgourmet vous retransmet les emails à l'adresse de votre choix, et dès que l'adresse email a expiré, tout mail envoyé à cette adresse est automatiquement avalé par Spamgourmet.com.

Cela permet de ne jamais donner sa vraie adresse email sur les sites.

Astuce : En créant une adresse email différente par site (très facile avec Spamgourmet), vous pouvez voir si le site a transmis votre adresse email à quelqu'un d'autre.

3.3.59 J'ai compris que le P2P (Peer-to-peer) est légal, mais que la majorité des fichiers qu'on y trouve sont illégaux

La technologie Peer-to-peer (P2P, partage de fichiers) n'est pas illégale, mais la majorité des internautes s'en servent pour partager des copies d'oeuvres protégées par le droit d'auteur, telle que des musiques (MP3), films (DivX, MPEG), livres, programmes piratés... et même de la pornographie infantile.

3.3.60 J'ai compris que le P2P est un nid à virus et qu'il est dangereux de télécharger des programmes venant de là

Un très grand nombre de programmes disponibles dans les réseaux P2P sont infectés par des virus ou contiennent un cheval de Troie. Evitez donc de récupérer des programmes de là. Allez plutôt les télécharger sur les sites des auteurs, c'est plus sûr.

3.3.61 J'ai compris que le MP3 et le DivX sont légaux, mais que que partager ma collection de CD ou toute autre oeuvre protégée par droits d'auteur est illégale, que ça soit par P2P ou tout autre moyen (HTTP, FTP...)

Le MP3 est légal. C'est une technologie développée entre autres par Thomson et de nombreuses applications commerciales utilisent ce système. DivX est un dérivé de MPEG4, qui est une technologie de compression vidéo tout à fait légale.

Mais ça ne veut pas dire que vous pouvez faire n'importe quoi avec !

Vous avez tout à fait le droit de copier votre collection de CD en MP3 pour l'écoute sur votre ordinateur, mais vous n'avez pas le droit de la partager avec d'autres personnes. Ni sur les réseaux P2P, ni autrement (site web HTTP, serveur FTP, email...).

3.3.62 J'ai compris qu'utiliser des logiciels piratés, crackés, déprotégés est non seulement illégal, mais aussi dangereux

Utiliser des logiciels piratés, non seulement c'est illégal, mais c'est dangereux.

Imaginez un antivirus piraté : Un inconnu vous a fourni un programme pour bidouiller l'antivirus afin de retirer sa protection. Qu'est-ce qui vous dit que cela n'a pas placé un cheval de Troie dans l'antivirus ? Ou bien que cela ne va pas faire buguer l'antivirus, réduisant ainsi votre protection ?

C'est dangereux, c'est illégal. Ne le faites pas.

De plus, on trouve de plus en plus de logiciels gratuits qui font aussi bien que les logiciels commerciaux. Quelques exemple :

- Photoshop ? Prenez *The Gimp*
- Microsoft Office ? Prenez *OpenOffice*
- 3D Studio Max ? Prenez *Blender*
- Norton Antivirus ? Prenez *Avast Home Edition*
- Norton Internet Security ? Prenez *ZoneAlarm*
- ACDSSee ? Prenez *XNView*
- Teleport Pro ? Prenez *HTTrack*
- CloneCD ? Prenez *BurnAtOnce*
- Nero ? Prenez *CD Burner XP Pro*
- WinZip ? Prenez *IZarc*

- PC Anywhere ? Prenez *VNC*
- FlashGet, GetRight ? Prenez *Free Download Manager*
- etc.

3.3.63 Je fais régulièrement des copies de sauvegarde de mes fichiers (sur CDR, sur un autre ordinateur, un autre disque dur, sur disquettes, sur clé USB...)

Si un virus ou un cheval de Troie détruit vos fichiers, vous serez bien content de pouvoir les récupérer.

Donc, faites une copie de sauvegarde de vos fichiers (aussi appelé backup) Il vous suffit de les copier sur un autre support, hors de l'ordinateur en temps normal (une clé USB, gravé sur CD, copié sur disquettes...). Pas besoin d'un programme spécial : il vous suffit de copier les fichiers. Bien sûr vous pouvez éventuellement les compresser pour gagner de la place, ou utiliser un logiciel de backup pour faire ça automatiquement.

Pas la peine de faire une copie des programmes eux-mêmes : vous pourrez les réinstaller en cas de problème. Sauvegardez seulement vos fichiers de travail.

Faites cette sauvegarde selon l'importance de vos fichiers : tous les jours, toutes les semaines ou tous les mois.

Astuce : pour ne pas oublier de fichier, organisez tous vos fichiers dans un même répertoire (par exemple Mes Documents). Comme ils sont tous à la même place, ça sera plus facile pour faire vos copies de sauvegarde.

Conseil : N'utilisez pas le logiciel de backup fourni avec Windows. Il arrive bien souvent qu'on ne puisse pas récupérer les fichiers d'une version de Windows à l'autre.

3.3.64 Je vérifie que je peux relire mes copies de sauvegarde

Après avoir fait une copie de sauvegarde, assurez-vous que vous arrivez bien à la relire. Un backup ne sert à rien si il est illisible.

3.3.65 Si j'ai une « box »(Freebox, LiveBox, C-Box, AOLBox...) et que l'option « Routeur »est disponible, je l'ai activée

La plupart des « box »proposées par les fournisseur d'accès possèdent une option « routeur »qui est désactivée par défaut.

Sans l'option routeur, la box n'est qu'un relais et devient « transparente ». Votre ordinateur est directement joignable d'internet. Il devient donc possible pour les pirates et virus de se connecter directement à votre ordinateur.

Avec le mode routeur, seule la box est accessible depuis internet. Elle fait office de relais entre votre ordinateur et internet et c'est elle qui va se connecter sur les serveurs internet à votre place. De plus elle bloquera toute tentative de connexion à votre ordinateur. C'est un avantage considérable : même en cas de défaillance de votre firewall, ou si votre firewall n'est pas à jour, la box bloquera les tentatives de connexion venant de l'extérieur.

Ça ne résout pas tous les problèmes, mais cela réduit notablement les risques.

Par exemple, chez le fournisseur d'accès Free, vous pouvez activer la fonction routeur de votre Freebox sur cette page : <http://fbxcfg.free.fr/routeur.html>

3.3.66 Si j'ai un routeur, j'ai changé le mot de passe par défaut du routeur

Si vous avez un routeur, ou un firewall « matériel », ils ont généralement un mot de passe par défaut réglé en usine.

Si vous ne le changez pas, un pirate pourrait en profiter pour l'utiliser et prendre le contrôle de votre routeur/firewall.

3.3.67 Si j'ai une connexion WiFi (ondes radio), j'ai activé la sécurité

Par défaut, la plupart des réseaux WiFi n'ont pas la sécurité activée (chiffrement). Cela veut dire que n'importe qui dans le voisinage *peut espionner vos communications et même utiliser votre connexion internet*. C'est vous qui serez tenu pour responsable si quelqu'un utilise votre connexion internet pour faire des choses illégales (piratage, pornographie infantile...).

Consultez la configuration de votre matériel pour activer le chiffrement.

Il existe 2 type de sécurisation : WEP et WPA (aussi appelé TKIP).

WEP est le strict minimum, mais vous devez savoir qu'il est loin d'être fiable à 100% (Il existe des méthodes pour pirater le WEP.) Tant que c'est possible, choisissez du matériel supportant WPA (nettement plus sûr).

Le piratage de réseaux WiFi est de plus en plus courant. Certains se promènent même en voiture à la recherche de réseaux WiFi ouverts.

Table des matières

1	Pourquoi sécuriser mon ordinateur, je n'ai rien à cacher !	2
2	Comment faire ?	2
2.1	WindowsUpdate : Je lance régulièrement WindowsUpdate et j'installe toutes les mises à jour critiques	3
2.2	Antivirus : J'ai un antivirus installé et il est mis à jour régulièrement	3
2.3	Firewall : J'ai un firewall installé, correctement configuré et qui est mis à jour quand c'est nécessaire	4
2.3.1	Configurer son firewall	5
2.3.2	Mettre à jour son firewall	5
2.4	Antispyware : J'ai un antispyware que je lance régulièrement et qui est mis à jour régulièrement	5
3	Pour aller plus loin... et être plus en sécurité	6
3.1	Checklist	6
3.2	Notes	8
3.3	Les explications en détail	9
3.3.1	J'ai compris qu'un ordinateur, c'est pas un réfrigérateur : c'est beaucoup plus compliqué	9
3.3.2	Je comprend que sans antivirus et sans firewall, je peux être infecté par un virus ou un cheval de Troie depuis des années sans sans m'en être aperçu	9
3.3.3	J'ai conscience que ne pas protéger mon ordinateur, c'est encourir des risques inutiles et contribuer au bordel ambiant	9
3.3.4	J'ai compris que je suis vulnérable même avec un modem 56K	9
3.3.5	Sur un nouvel ordinateur (ou un ordinateur sur lequel je viens de ré-installer Windows), j'installe un firewall avant ma première connexion à internet.	10
3.3.6	J'ai compris qu'il n'existe aucun logiciel (antivirus, firewall ou autre) qui assure une sécurité à 100%, mais que ces logiciels restent nécessaires	10
3.3.7	J'ai compris que j'ai les moyens de me protéger gratuitement, et que la seule chose que ça me coûtera, c'est du temps et de réflexion	10
3.3.8	J'ai compris que les logiciels, c'est comme le sexe : c'est pas parce que c'est payant que c'est meilleur	11
3.3.9	Je sais utiliser mon antivirus et le configurer. J'en ai lu la documentation	11
3.3.10	J'ai compris que je suis responsable aux yeux de la loi de ce qui est fait avec ma connexion internet	11
3.3.11	J'ai compris que je ne suis pas anonyme sur internet : mon fournisseur d'accès sait qui je suis et peut fournir aux autorités mon identité et adresse	12
3.3.12	J'ai compris que je ne suis anonyme sur internet que tant que je ne donne pas d'informations personnelles, sur un site web ou ailleurs	12
3.3.13	J'ai compris que les adresses d'expéditeur d'email peuvent être totalement falsifiées	12
3.3.14	Je n'envoie jamais la moindre information confidentielle (mot de passe, numéro de carte de crédit...) à ma banque, mon fournisseur d'accès ou toute autre entreprise qui me le demande (Microsoft y compris)	12

3.3.15	Je n'ouvre jamais les attachements dont je n'attend pas la réception, même s'ils proviennent de mon FAI, Microsoft, ou même <i>de mes propres amis</i>	13
3.3.16	Je sais configurer Internet Explorer et Outlook Express pour désactiver ActiveX et l'active scripting (VBScript, Javascript, WSH...)	13
3.3.17	Je ne clique pas bêtement sur tout fichier que je trouve	13
3.3.18	Je ne lance pas les programmes 'marrants', mêmes envoyés par des amis ou des connaissances	14
3.3.19	Un ami qui place un cheval de Troie sur mon ordinateur n'est pas un ami	14
3.3.20	Quand je choisis un logiciel à télécharger, je m'assure d'abord qu'il ne contient pas de spyware	14
3.3.21	Quand je télécharge un programme que je veux installer, je le télécharge toujours d'une source sûre, et si possible directement du site de l'auteur	14
3.3.22	Je veille à ce que la fonction de mise à jour automatique de mon antivirus/firewall/antispyware soit activée et qu'elle fonctionne	15
3.3.23	Si la mise à jour automatique de mon antivirus / firewall / antispyware ne fonctionne pas, je sais où aller télécharger la mise à jour et comment l'installer manuellement	15
3.3.24	Je sais quels programmes sont lancés au démarrage de mon ordinateur et je n'ai laissé que ceux dont j'ai absolument besoin	15
3.3.25	J'ai désactivé tous les services dont je n'ai pas besoin (Windows NT / 2000 / XP / 2003 uniquement)	16
3.3.26	J'ai désactivé le partage de fichiers Windows	16
3.3.27	Si j'utilise le partage de fichiers, je ne partage jamais de dossier sans mot de passe	16
3.3.28	J'ai désactivé l'utilisateur invité (guest). (Windows NT / 2000 / XP / 2003 uniquement)	17
3.3.29	J'ai désactivé le partage par défaut des disques. (Windows NT / 2000 / XP / 2003 uniquement)	17
3.3.30	Je ne travaille pas en tant qu'administrateur (Windows NT / 2000 / XP / 2003 uniquement)	17
3.3.31	Je choisis de bons mots de passe	17
3.3.32	Si j'ai des serveurs installés sur mon ordinateur (serveur web (HTTP), FTP, ssh...), je sais les configurer et je les ai correctement configurés	18
3.3.33	Si j'ai des serveurs installés sur mon ordinateur, je les met à jour régulièrement	18
3.3.34	Je n'utilise pas des logiciels en version beta. Je n'utilise que les versions stables	18
3.3.35	Je surveille l'actualité informatique et je réagis en conséquence (patches, mises à jour des logiciels, etc...)	18
3.3.36	Je ne désactive jamais mon antivirus, même quand j'insère le CD, la disquette ou la clé USB d'un ami qui m'assure qu'il ne peut y avoir de virus dessus	18
3.3.37	Je sais ce que sont les hoax et je ne me fais pas avoir	18
3.3.38	Je sais ce que sont les scam et je ne me fais pas avoir	19
3.3.39	Je sais ce que sont les spams et je ne me fais pas avoir	19
3.3.40	J'ai compris quand un programme est censé aller sur internet ou non	19
3.3.41	J'ai compris ce que sont les tentatives de connexion à mon ordinateur venant d'internet	19

3.3.42	J'ai compris ce qu'était le mode apprentissage de mon firewall et je sais le désactiver	20
3.3.43	En cas de doute, je sais comment neutraliser ma connexion internet (avec le firewall ou sans)	20
3.3.44	Je ferme toujours ma connexion à internet quand je n'en ai pas besoin . .	20
3.3.45	Dans Internet Explorer, je ne clic jamais bêtement 'oui' sur toutes les fenêtres de confirmation qui s'affichent	21
3.3.46	J'ai toujours sous la main l'adresse un forum où je sais que je peux aller demander de l'aide ou des renseignements	21
3.3.47	J'ai toujours sous la main les coordonnées d'un ami « qui s'y connaît en informatique » et qui peut me dépanner en cas de problème	21
3.3.48	J'ai conscience que l'intelligence collective d'un forum est meilleure conseillère que l' « ami qui s'y connaît en informatique »	21
3.3.49	J'ai toujours sous la main les URL des antivirus en ligne. On ne sait jamais, ça peut servir	22
3.3.50	Je sais désactiver la restauration système en cas de problème	22
3.3.51	J'ai configuré l'explorateur de Windows pour afficher les extensions de fichiers et fichiers/répertoires cachés	22
3.3.52	J'ai toujours à portée de main le CD d'installation de Windows, le numéro de série, les pilotes de chacun de mes périphériques (y compris du modem internet), le CD d'installation de mon fournisseur d'accès et les codes d'accès	23
3.3.53	J'ai au moins une disquette qui me permet de démarrer mon ordinateur dessus et accéder au lecteur de CD-Rom. J'ai vérifié que cette disquette fonctionne bien et que je peux accéder au lecteur de CD-Rom	23
3.3.54	J'ai une connexion internet de secours (vieux modem téléphonique, autre ordinateur, ami, voisin)	23
3.3.55	Je ne répond jamais au spam. Je n'essaie pas de me désinscrire	23
3.3.56	Quand je dois entrer des informations confidentielles (ex : numéro de carte de crédit), je le fais uniquement dans des pages sécurisés (HTTPS), et pas sur un obscure site web	24
3.3.57	Quand un site me demande mon adresse email, j'évite de lui donner, surtout si ils me promettent des choses gratuitement	24
3.3.58	J'utilise Spangourmet.com pour recevoir des mails des sites qui me demandent mon adresse email	24
3.3.59	J'ai compris que le P2P (Peer-to-peer) est légal, mais que la majorité des fichiers qu'on y trouve sont illégaux	25
3.3.60	J'ai compris que le P2P est un nid à virus et qu'il est dangereux de télécharger des programmes venant de là	25
3.3.61	J'ai compris que le MP3 et le DivX sont légaux, mais que que partager ma collection de CD ou toute autre oeuvre protégée par droits d'auteur est illégale, que ça soit par P2P ou tout autre moyen (HTTP, FTP...) . .	25
3.3.62	J'ai compris qu'utiliser des logiciels piratés, crackés, déprotégés est non seulement illégal, mais aussi dangereux	25
3.3.63	Je fais régulièrement des copies de sauvegarde de mes fichiers (sur CDR, sur un autre ordinateur, un autre disque dur, sur disquettes, sur clé USB...) 26	26
3.3.64	Je vérifie que je peux relire mes copies de sauvegarde	26

3.3.65	Si j'ai une « box »(Freebox, LiveBox, C-Box, AOLBox...) et que l'option « Routeur »est disponible, je l'ai activée	26
3.3.66	Si j'ai un routeur, j'ai changé le mot de passe par défaut du routeur . . .	27
3.3.67	Si j'ai une connexion WiFi (ondes radio), j'ai activé la sécurité	27

À propos de ce document

Ce document, Safe-Hex, est disponible en version originale et mise à jour sur <http://www.sebsauvage.net/safehex.html>. Il a été écrit par Sébastien Sauvage (<http://www.sebsauvage.net>) et mis en page par Simon Plante (<http://www.blogsimonpca.ca.cx>) selon la version du 30 octobre 2005.

Il a été placé par son auteur dans le domaine libre, ce qui vous permet de le distribuer, le copier et le modifier librement. Cette mise en page aussi est placée dans le domaine public.

Vous êtes encouragés à distribuer ce document à tous vos amis.

Ce document à, dans sa version originale, été vaguement inspiré par <http://www.securityfocus.com/columnists/220>.