« *Pourquoi sécuriser mon ordinateur ? Je n'ai rien à cacher !* » - Il y a de très bonnes raisons !

L'indispensable

pour tout utilisateur de Windows connecté à internet

WindowsUpdate

Installez les mises à jour de sécurité de Windows avec WindowsUpdate.

Firewall

Installez un firewall pour bloquer les connexions réseau venant d'internet.

Antivirus

Installez un antivirus pour contrer les virus.

Antispyware

Installez un antispyware pour éliminer les logiciels-espion.

Recommandé

pour une meilleure sécurité, et un surf plus rapide et efficace

Firefox

Un navigateur plus sûr et plus pratique qu'Internet Explorer.

WOT (Web Of Trust)

Vous protège des sites douteux.

OpenDNS

Protection contre les sites de phishing et accélération de la navigation.

Thunderbird

Un logiciel d'email plus sûr que Outlook Express et qui peut éliminer le spam.

Pour aller plus loin...

et être encore 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 appellé «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 comprendre un point précis ? Vous voulez en savoir plus ? Pas de panique !
Consultez les liens que je vous donne: http://sebsauvage.net/safehex.html#liens
(Merci de ne pas me poser de questions par mail.)

L'indispensable pour internet

- [ ] J'ai compris qu'un ordinateur, c'est pas un réfrigérateur: c'est beaucoup plus compliqué.
(Pourquoi ?)

- [ ] 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.
(Pourquoi ?)

- [ ] J'ai conscience que ne pas protéger mon ordinateur, c'est encourir des risques inutiles et contribuer au bordel ambiant.
(Pourquoi ?)

- [ ] J'ai compris que je suis vulnérable même avec un modem 56K.
(Pourquoi ?)

- [ ] 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.
(Pourquoi ?)

- [ ] 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.
(Pourquoi ?)

- [ ] 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.
(Pourquoi ?)

- [ ] J'ai compris que les logiciels, c'est comme le sexe: c'est pas parceque c'est payant que c'est meilleur.
(Pourquoi ?)

- [ ] Je sais utiliser mon antivirus et le configurer. J'en ai lu la documentation.
(Pourquoi ?)

- [ ] J'ai compris que je suis responsable aux yeux de la loi de ce qui est fait avec ma connexion internet.
(Pourquoi ?)

- [ ] 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.
(Pourquoi ?)

- [ ] J'ai compris que je ne suis pas anonyme sur internet que tant que je ne donne pas d'informations personnelles, sur un site web ou ailleurs.
(Pourquoi ?)

- [ ] J'ai compris que les adresses d'expéditeur d'email peuvent être totalement falsifiées.
(Pourquoi ?)

- [ ] 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).
(Pourquoi ?)

- [ ] 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* .
(Pourquoi ?)

- [ ] Je sais configurer Internet Explorer et Outlook Express pour désactiver ActiveX et l'active scripting (VBScript, Javascript, WSH...)
(Pourquoi ?)

- [ ] Je ne clic pas bêtement sur tout fichier que je trouve.
(Pourquoi ?)

- [ ] Je ne lance pas les programmes 'marrants', mêmes envoyés par des amis ou des connaissances.
(Pourquoi ?)

- [ ] Un ami qui place un cheval de Troie sur mon ordinateur n'est pas un ami.
(Pourquoi ?)

- [ ] Quand je choisis un logiciel à télécharger, je m'assure d'abord qu'il ne contient pas de spyware.
(Pourquoi ?)

- [ ] 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.
(Pourquoi ?)

- [ ] Je veille à ce que la fonction de mise à jour automatique de mon antivirus/firewall/antispyware soit activée et qu'elle fonctionne.
(Pourquoi ?)

- [ ] 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.
(Pourquoi ?)

- [ ] Je sais quels programmes sont lancés au démarrage de mon ordinateur et je n'ai laissé que ceux dont j'ai absolument besoin.
(Pourquoi ?)

- [ ] J'ai désactivé tous les services dont je n'ai pas besoin (Windows NT/2000/XP/2003 uniquement).
(Pourquoi ?)

- [ ] J'ai désactivé le partage de fichiers Windows.
(Pourquoi ?)

- [ ] Si j'utilise le partage de fichiers, je ne partage jamais de dossier sans mot de passe.
(Pourquoi ?)

- [ ] J'ai désactivé l'utilisateur invité (guest). (Windows NT/2000/XP/2003 uniquement).
(Pourquoi ?)

- [ ] J'ai désactivé le partage par défaut des disques. (Windows NT/2000/XP/2003 uniquement).
(Pourquoi ?)

- [ ] Je ne travaille pas en tant qu'administrateur (Windows NT/2000/XP/2003 uniquement).
(Pourquoi ?)

- [ ] Je choisis de bons mots de passe.
(Pourquoi ?)

- [ ] Je met à jour les logiciels installés sur mon ordinateur.
(Pourquoi ?)

- [ ] Si j'ai des serveurs installés sur mon ordinateur, je les met à jour régulièrement.
  (Pourquoi ?)
- [ ] Je n'utilise pas des logiciels en version beta. Je n'utilise que les versions stables.
  (Pourquoi ?)
- [ ] Je surveille l'actualité informatique et je réagis en conséquence (patchs, mises à jour des logiciels, etc...)
  (Pourquoi ?)
- [ ] 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.
  (Pourquoi ?)
- [ ] Je sais ce que sont les hoax et je ne me fais pas avoir.
  (Pourquoi ?)
- [ ] Je sais ce que sont les scam et je ne me fais pas avoir.
  (Pourquoi ?)
- [ ] Je sais ce que sont les spams et je ne me fais pas avoir.
  (Pourquoi ?)
- [ ] Je sais interpréter les alertes de mon firewall.
  - [ ] J'ai compris quand un programme est censé aller sur internet ou non.
    (Pourquoi ?)
  - [ ] J'ai compris ce que sont les tentatives de connexion à mon ordinateur venant d'internet.
    (Pourquoi ?)
  - [ ] J'ai compris ce qu'était le mode apprentissage de mon firewall et je sais le désactiver.
    (Pourquoi ?)
- [ ] En cas de doute, je sais comment neutraliser ma connexion internet (avec le firewall ou sans).
  (Pourquoi ?)
- [ ] Je ferme toujours ma connexion à internet quand je n'en ai pas besoin.
  (Pourquoi ?)
- [ ] Dans Internet Explorer, je ne clic jamais bêtement 'oui' sur toutes les fenêtres de confirmation qui s'affichent.
  (Pourquoi ?)
- [ ] J'ai toujours sous la main l'adresse un forum où je sais que je peux aller demander de l'aide ou des renseignements.
  (Pourquoi ?)
- [ ] J'ai toujours sous la main les coordonnées d'un ami «qui s'y connait en informatique» et qui peut me dépanner en cas de problème.
  (Pourquoi ?)
- [ ] J'ai conscience que l'intelligence collective d'un forum est meilleure conseillère que l'«ami qui s'y connaît en informatique».
  (Pourquoi ?)
- [ ] J'ai toujours sous la main les URL des antivirus en ligne. On ne sait jamais, ça peut servir.
  (Pourquoi ?)
- [ ] Je sais désactiver la restauration système en cas de problème.
  (Pourquoi ?)
- [ ] J'ai configuré l'explorateur de Windows pour afficher les extensions de fichiers et fichiers/répertoires cachés.
  (Pourquoi ?)
- [ ] 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.
  (Pourquoi ?)
- [ ] 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.
  (Pourquoi ?)
- [ ] J'ai une connexion internet de secours (vieux modem téléphonique, autre ordinateur, ami, voisin).
  (Pourquoi ?)
- [ ] 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.
  (Pourquoi ?)
- [ ] Je ne répond jamais au spam. Je n'essaie *pas* de me déinscrire.
  (Pourquoi ?)
- [ ] 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.
  (Pourquoi ?)
- [ ] Quand un site me demande mon adresse email, j'évite de la donner, surtout s'ils me promettent des choses gratuitement.
  (Pourquoi ?)
- [ ] J'utilise Spamgourmet.com pour recevoir des mails des sites qui me demandent mon adresse email.
  (Pourquoi ?)
- [ ] J'ai compris que le P2P (Peer-to-peer) est légal, mais que la majorité des fichiers qu'on y trouve sont illégaux.
  (Pourquoi ?)
- [ ] J'ai compris que le P2P est un nid à virus et qu'il est dangereux de télécharger des programmes venant de là.
  (Pourquoi ?)
- [ ] 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...)
  (Pourquoi ?)
- [ ] J'ai compris qu'utiliser des logiciels piratés, crackés, déprotégés est non seulement illégal, mais aussi dangereux.
  (Pourquoi ?)

- ☐ 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...)
  (Pourquoi ?)
- ☐ Je vérifie que je peux relire mes copies de sauvegarde.
  (Pourquoi ?)
- ☐ Si j'ai une "box" (Freebox, LiveBox, C-Box, AOLBox...) et que l'option "Routeur" est disponible, je l'ai activée.
  (Pourquoi ?)
- ☐ Si j'ai un routeur, j'ai changé le mot de passe par défaut du routeur.
  (Pourquoi ?)
- ☐ Si j'ai une connexion WiFi (ondes radio), j'ai activé la sécurité.
  (Pourquoi ?)

Explications détaillées

pour tout comprendre

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.

Dans la majorité des cas, **les pirates ne s'intéressent pas à ce qu'il y a sur votre disque dur. Ce qui les intéressent, c'est votre connexion internet.**
S'ils font des choses illégales avec leur connexion internet, ils se feront attraper. Par contre, s'il utilisent votre connexion internet comme relai, ils seront à l'abris: C'est vous qui prendrez.

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 nombres 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 cyberespace, *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 relais: 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.

Un exemple ? Cet homme (article en anglais) avait été accusé de pédophilie car son ordinateur - piraté - avait téléchargé des images pédophiles à son insue. Après examen par des experts, il a été acquitté, mais sa vie a été un enfer pendant des mois, il a perdu son travail et tous ses amis ont fuit. Et ce n'est pas le premier internaute à subir les conséquences d'un ordinateur mal sécurisé.

WindowsUpdate

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 et en prendre le contrôle.
Il est donc important de les corriger.

A titre d'exemple: Microsoft a corrigé une faille de sécurité en octobre 2008. Beaucoup d'internautes n'ont pas installé cette mise à jour. Résultat: **9 millions de PC infectés** fin janvier 2009 par le virus *Conficker* (aussi appellé *Downadup*) qui utilisait justement cette faille pour se propager.

Comment ?

Microsoft fourni régulièrement des mises à jour pour Windows.
Windows est fourni avec un programme qui télécharge et installe facilement les mises à jour: C'est **WindowsUpdate**.

En principe, WindowsUpdate est déjà actif sur votre ordinateur et installe automatiquement les mises à jour.
Si ce n'est pas le cas (ou pour vérifier), lancez Internet Explorer et allez sur http://windowsupdate.microsoft.com et laissez-vous guider.

Il n'est pas recommandé d'utiliser un système d'exploitation pour lequel l'éditeur ne corrige plus les failles, car cela permet aux pirates et virus d'infecter plus facilement l'ordinateur.

Or:

- Microsoft ne fournit plus de mises à jour de sécurité pour Windows 95, 98, ME, NT4 et 2000. Vous ne devriez plus utiliser ces systèmes.
- A partir d'**avril 2014**, Microsoft ne corrigera plus les bugs découverts dans Windows XP.
- A partir de **juillet 2010**, Microsoft ne corrigera plus les bugs découverts dans Windows XP SP1 et SP2. Je vous recommande chaudement d'installer le SP3 (soit à l'aide de WindowsUpdate, soit en le téléchargeant sur le site de Microsoft (environ 324 Mo)).

Pensez également à mettre vos logiciels à jour

Une vieille version de *Flash* ou *Acrobat PDF Reader* peut permettre l'infection de votre ordinateur **simplement en affichant une page web**.

Pour mettre à jour Flash:

- Téléchargez ces deux fichiers:
  - http://fpdownload.adobe.com/get/flashplayer/current/install_flash_player_ax.exe
  - http://fpdownload.adobe.com/get/flashplayer/current/install_flash_player.exe

- Fermez tous vos navigateurs.
- Installez ces deux programmes.

Pour les autres logiciels, il vous faudra vérifier - logiciel par logiciel - s'il existe une version plus récente et l'installer.
Le logiciel gratuit ***Secunia PSI*** peut vous aider à trouver les vieilles version dangereuses des logiciels et vous donner les liens pour les mettre à jour.

Firewall

Pourquoi ?

Quand un ordinateur est connecté à internet, il peut communiquer avec d'autres ordinateurs pour envoyer et recevoir des informations.
Cela veut dire que d'autres ordinateurs ont la possibilité de se connecter sur le vôtre. En exploitant des failles de sécurité, il devient alors possible de prendre à distance le contrôle de votre ordinateur, sans que vous vous en rendiez compte.

WindowsUpdate permet de corriger les failles connues qui permettraient de prendre le contrôle de votre ordinateur, mais quid des failles encore non découvertes ?

Il est donc important d'empêcher qui que ce soit de se connecter à distance sur votre ordinateur: C'est le rôle du firewall.

Comment ?

Le firewall est un logiciel qui va contrôler qui vient se connecter, et bloquer les connexions non autorisées en fonction de règles que vous aurez vous-même choisies.

Windows XP (SP2 uniquement !), Windows Vista et **Windows 7** possèdent un firewall intégré qui est actif dès l'installation.
Pour les autres (ce qui inclue Windows XP sans le SP2), il est impératif d'installer un firewall. On en trouve des gratuits, comme *ZoneAlarm* ou *Jetico Personal Firewall*. (Ces firewalls peuvent également être installé dans Windows Vista et Windows XP SP2.)

Certains firewalls peuvent également contrôler **quels logiciels ont le droit d'envoyer et recevoir des informations** sur internet.
Cela permet de repérer et bloquer un logiciel frauduleux ou un cheval de Troie qui aurait été "greffé" à un logiciel anodin (tel qu'un logiciel de dessin).

Quel firewall choisir ?

ZoneAlarm reste un bon choix. Il est totalement gratuit et relativement fiable.

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.

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.

Antivirus

Pourquoi ?

Les virus sont des programmes malveillants qui s'installent sur votre ordinateur sans votre consentement et font diverses choses malsaines, comme voler vos mots de passe, vos fichiers, donner l'accès à votre ordinateur à d'autres personnes, envoyer du spam, propager des virus ou attaquer d'autres ordinateurs.

Il existe des **centaines de milliers de virus**. Il est humainement impossible de connaître tout ces virus et les contrer

Comment ?

Installez un antivirus (on en trouve des gratuits).
C'est le rôle des antivirus de détecter ces programmes malveillants et les bloquer avant qu'ils n'infectent votre ordinateur.

La plupart des antivirus vérifient automatiquement tout fichier que vous essayez d'ouvrir: Par exemple, si vous double-cliquez sur un fichier Word pour l'ouvrir, l'antivirus vérifiera que le fichier Word est sain avant de laisser Word accéder au fichier. L'antivirus vous préviendra de toute infection trouvée.

N'oubliez pas qu'aucun antivirus n'est efficace à 100%.
L'antivirus est la ceinture de sécurité de l'ordinateur: Ça ne garantie pas que vous n'aurez pas d'accident, mais ça peut vous sauver la vie dans beaucoup de cas.

Quel antivirus choisir ?

Vous pouvez prendez *Avast Edition Familiale* (en français) ou *Antivir Personal Edition* (en français aussi).

Mettre à jour son antivirus

Chaque antivirus possède une sorte de dictionnaire des virus, appellé *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 la majorité des antivirus font même cela automatiquement, ce qui est encore plus pratique.

Antispyware

Pourquoi ?

En plus des virus, il existe une quantité phénomale d'autres programmes malveillants:

- Les chevaux de Troie, qui permettent à des pirates de savoir tout ce que vous faites, voler vos mots de passe et prendre le contrôle total de votre ordinateur,
- Les spywares, les logiciels créés par des entreprises peu scupuleuses qui espionnent vos habitudes afin d'exploiter commercialement ces informations,
- Les adwares, des logiciels qui affichent des publicités non sollicitées,
- Les dialers, des programmes qui forcent votre modem à composer des numéros surtaxés,
- et beaucoup d'autres.

Il est courant que ces logiciels soient "greffés" à des logiciels qui semblent anodins, ou même ajouté à des logiciels et jeux piratés.

Les antivirus ne détectent pas tous les types de logiciel malveillants. Ce sont les antispywares qui vous permettent de traquer et éliminer spécifiquement ces programmes malveillants.

Comment ?

Installez un antispyware et lancez une vérification par l'antispyware une fois par semaine.

Quel antispyware choisir ?

Spybot Search & Destroy et *MalwareBytes* sont de bons antispywares gratuits.

Mettre à jour son antispyware

De même que pour les antivirus, les antispywares possède une base de signatures qu'il faut mettre à jour de temps en temps. Pensez à le faire une fois par semaine, avant de lancer la vérification.

Par exemple, pour Spybot S&D, voici la procédure à suivre.

Firefox

Internet Explorer 6 est un bien mauvais navigateur et pose de nombreux problèmes de sécurité. Internet Explorer 7 et 8 sont déjà meilleurs qu'IE6, mais on peut faire bien mieux: Installer **Firefox**.
Non seulement Firefox est **plus sûr**, mais il est également **beaucoup plus pratique**.

Si Firefox ne vous plaît pas, **Opera** et **Google Chrome** sont une alternative.

WOT (Web Of Trust)

WOT (Web Of Trust) est une petite extension (un petit programme) qu'on peut ajouter à Firefox, Internet Explorer ou Google Chrome et qui vous signalera immédiatement **les sites douteux**: commerçants véreux, faux sites de banques, arnaques, faux-antivirus, faux-antispywares, sites contenant des virus, sites de téléchargement distribuant des fichiers infectés, etc.
WOT se base sur les rapports des internautes eux-mêmes, ainsi que sur plusieurs sources réputées pour lutter contre les arnaques et fraudes sur internet (PhishTank, SpamCop, DNS-BH, MalwarePatrol, etc.)

WOT est gratuit, ne nécessite aucune connaissance et vous protègera contre une incroyable quantité de sites malveillants.
Installez-le ! Un jour où l'autre, croyez-moi, vous serez content de l'avoir fait.

Toutes les instructions sont là: http://www.commentcamarche.net/faq/sujet-15620-wot-web-of-trust-essentiel-pour-l-internaute-avise

OpenDNS

Les DNS, ce sont les serveurs qui convertissent une adresse (www.commentcamarche.net) en adresse IP (194.169.240.130).
Vous utilisez les serveurs DNS de votre fournisseur d'accès, mais vous avez la possibilité d'utiliser gratuitement les serveurs d'OpenDNS. Cela offre de nombreux avantages, les deux premiers étant:

- Une protection anti-phishing: OpenDNS bloque les sites qui essaient d'imiter les sites des banques, eBay, etc. afin d'éviter de vous faire arnaquer.
- OpenDNS est très rapide, ce qui permet (dans la majorité des cas) de surfer plus vite.

Des options supplémentaires vous permettent de filtrer les sites adultes, etc.
Vous trouverez plus d'informations dans cet article.

Thunderbird

Outlook Express est un logiciel d'email fourni avec Windows. Il n'est pas très performant, et il a par le passé posé de **nombreux problèmes de sécurité**.
On peut sans problème le remplacer par **Thunderbird**. Parmis ses avantages:

- Plus pratique
- Peut gérer plusieurs comptes mail
- Sait filtrer le spam (emails publicitaires non sollicités).

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.

Retour

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.

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.

Retour

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 pillule 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 relais au spam.

Pour vous protéger: Notre carré magique (windowsupdate+antivirus+firewall+antispyware) devrait bloquer 99,99% des tentatives de piratage.

Retour

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. Le virus se moque bien du type deconnexion que vous utilisez.

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

Retour

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.

Si vous avez Windows Vista ou Windows XP équipé du service pack 2 (SP2), alors vous avez déjà un firewall.

Retour

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.

Retour

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 antispywares gratuits et d'excellente qualité !

Sécuriser votre ordinateur vous demandera un peu de temps, de réflexion, peut-être aussi d'énervement, 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.

Retour

J'ai compris que les logiciels, c'est comme le sexe: c'est pas parceque 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'assoir 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.

Retour

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.

Retour

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.

Retour

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.

Soyez responsable.

Retour

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.

Retour

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 et spammeurs font également très souvent ce genre de chose.

Soyez donc méfiant.

Retour

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.

Retour

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, patchs, correctifs ou antivirus par email. Il faut toujours les téléchager 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 quelquechose que vous vous attendiez à recevoir.

Retour

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

Microsoft a inclu 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), ou mieux, de **laisser tomber Internet Explorer** au profit de meilleurs navigateurs comme **Firefox**.

Retour

Je ne clic 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.

Retour

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.

Retour

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 crûement: Vous êtes à poil sur internet.

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

Retour

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.

Retour

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 Firefox uniquement sur le site mozilla.com. 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...)

Retour

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.

Retour

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.

Pour savoir comment faire, voir cet article sur Commentcamarche.net.

Retour

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 programme pour pénétrer dans votre ordinateur.
Comme certains de ces programmes ouvrent des ports en écoute (sur votre connexion internet), arrêter ces programme 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 *AutoRuns* (http://sebsauvage.net/logiciels/autostartmanager.html) peuvent vous aider à voir quels sont les programmes lancés au démarrage et les désactiver.

Retour

J'ai désactivé tous les services dont je n'ai pas besoin (Windows NT/2000/XP/2003/Vista 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.

Retour

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.
Malheureusent, 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.

Retour

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.

Retour

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

Retour

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

Retour

Je ne travaille pas en tant qu'administrateur (Windows NT/2000/XP/2003/Vista 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.

Retour

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 possible (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: "**L**a **m**ère **m**ichèle **n**'a **p**as **p**erdu **s**on **c**hat **b**otté" ---> `lmmnppscb$77`

Retour

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 restreind 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.

Retour

Je met à jour les logiciels installés sur mon ordinateur.

Des failles sont régulièrement découvertes dans divers logiciels. Certaines de ces failles pourraient permettre le piratage de votre ordinateur.
Par exemple, utiliser une vieille version du plugin Flash (qui permet de faire des pages web animées) permet à un pirate de prendre le contrôle de votre ordinateur simplement vous incitant à afficher une simple page web.

Tenez-vous au courant mettez promptement à jour vos différents logiciels quand des failles sont découvertes.
Des logiciels peuvent vous y aider, comme:

- *Secunia Personal Software Inspector*
- *FileHippo.com Update Checker*
- *Software Informer*

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.

Retour

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.

Retour

Je surveille l'actualité informatique et je réagis en conséquence (patchs, 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 Secuser.com, CERT.org, SANS.org, etc.

En suivant l'actualité ainsi, vous pourrez prendre les mesures nécessaire 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.

Retour

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.

Retour

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.

Retour

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.

Retour

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 passports, d'autres papier officiels, des crédits, des logiciels, du matériel informatique, des cartouches d'encre, des pillules 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.

Retour

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 !

Retour

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 essai de communiquer avec vous.
Cela arrive souvent, voir 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 parceque vous avez récupéré l'adresse IP de quelqu'un qui vient de se déconnecter, ou bien parcequ'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 dir 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/.

Retour

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).

Retour

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

Si vous décelez une activité suspect 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 traffic". Cela neutralise toutes les communications entrantes et sortantes.

Un second clic vous permet réactiver les communications.

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

Retour

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 risque pour rien.

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

Retour

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.

Retour

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...

Retour

J'ai toujours sous la main les coordonnées d'un ami "qui s'y connait 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.

Retour

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 connait en informatique".

Retour

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.

Antivirus en ligne pour scanner un ordinateur, un disque, un répertoire:

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

Adresse	Moteur d'antivirus	Désinfecte ?	Remarques
http://www.bitdefender.com	BitDefender	oui	Cliquez sur le lien "Free Online Scanner" en bas de page.
http://www.f-secure.com/en_EMEA/security/security-lab/tools-and-services/online-scanner	F-Secure	oui	Cocher la case "I have read..." et cliquer sur "Run Check".
http://www.pandasecurity.com/activescan/index/	Panda	oui, si vous vous inscrivez (inscription gratuite)	Cliquer sur le bouton "Analyser"
http://onecare.live.com/site/fr-fr/center/howsafe.htm	Microsoft OneCare	oui	Cliquez sur "Analyse antivirus". Désinfecte mais n'indique pas quel était le problème.
http://cainternetsecurity.net/entscanner/	ComputerAssociates	oui	Cliquez sur le bouton "Start scan".
http://www.emsisoft.com/en/software/ax/?scan=1	a-Squared	oui	Plutôt orienté cheveaux de troie/keyloggers/spywares que virus.
http://www.eset.com/onlinescan/	eSet NOD32	oui	Cochez "YES, I accept the Terms of Use." et cliquez sur "Start"
http://www.kaspersky.com/virusscanner	Kaspersky	non	Cliquer sur le bouton "Kasperksy Online Scanner"
http://security.symantec.com/sscv6/vc_scan.asp	Norton / Symantec	non	Choisir "I accept" et cliquer sur "Next"
http://home.mcafee.com/Downloads/FreeScan.aspx	McAfee	non	Cliquer sur "Analyser maintenant"

Notes:

- Certains de ces antivirus en ligne ne sont pas capables de désinfecter (par exemple Kaspersky en ligne détecte mais ne désinfecte pas. Par contre, BitDefender désinfecte.)
- Il arrive que certains virus bloquent les accès aux sites antivirus. Dans ce cas, essayez d'autres antivirus en ligne.

Antivirus à télécharger pour scanner un ordinateur, un disque, un répertoire:

Ces antivirus sont à télécharger pour scanner votre ordinateur. Attention: ils ne fournissent pas de protection en temps réel mais peuvent être utiles pour une analyse ponctuelle. Notez que les antivirus qui fonctionnent sans connexion internet peuvent être emportés sur clé USB pour scanner des PC n'ayant pas de connexion internet.
Notez également que certains doivent être intégralement re-téléchargés pour avoir les dernières bases de signature (comme DrWeb Cureit).
Ces logiciels ne nécessitent pas un navigateur particulier.

Logiciel	Page web	Moteur d'antivirus	Lien téléchargement direct	Fonctionne sans connexion internet	Désinfecte	Mise à jour	Remarques

Dr.Web CureIt!	http://www.freedrweb.com/cureit/	Dr. Web	Lien	oui	oui	retélécharger	-
McAfee Stinger	http://vil.nai.com/vil/stinger/	McAfee	Voir page web	oui	oui	retélécharger	Ne détecte que les virus les plus courants (environ 3000).
TrendMicro Housecall	http://housecall.trendmicro.com/fr/	TrendMicro	32 bits 64 bits	non*	oui	relancer	Par défaut, ne scanne pas "Mes documents". La mise à jour des signatures nécessite une connexion internet.
PrevX CSI Free	http://www.prevx.com/	PrevX	Lien	non	non	relancer	Par défaut, scanne seulement les zones système courantes. Pour scanner un dossier/fichier précis, utiliser le clic-droit dans l'explorateur de fichiers Windows. ***Attention: Il ne détecte pas les virus si la connexion internet ne marche pas ! (Aucune alerte)***

* semble planter à la fin du scan si la connexion internet n'est pas présente. Il est alors impossible de consulter le rapport d'infection et de désinfecter.

Pour scanner un seul fichier:

Si vous avez juste un fichier douteux à scanner, vous pouvez utiliser un des sites suivants: Ils testeront votre fichier avec plusieurs antivirus à la fois.
Cela fonctionne avec n'importe quel navigateur.

Adresse	Taille max fichier	Nombre d'antivirus utilisés
http://virustotal.com	?	40
http://virscan.org	10 Mo	37
http://scanner.virus.org	5 Mo	23
http://virusscan.jotti.org	10 Mo	20
http://viruschief.com	?	10
http://filterbit.com	20 Mo	9

(données au 31 mars 2009)

Retour

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 certains 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 site. 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.

Retour

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.

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

Retour

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'inscruster 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 nécessaire pour réparer.

Retour

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.

Les CD d'installation de Windows XP et Windows Vista sont bootables: C'est à dire que vous pouvez l'insérer dans votre ordinateur et démarrer directement dessus pour réinstaller Windows, même si Windows ne démarre plus correctement sur disque dur.

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 possède un outil pour créer cette disquette, et on trouve également des disquettes bootables sur internet:

- http://www.bootdisk.com/
- 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.

Retour

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.

Retour

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.

Si moins de 1% des internautes qui reçoivent un spam répondent, le spam reste rentable pour les spammeurs.
Ne jouez pas leur jeu. N'achetez jamais ce qu'on vous propose par email.
De toute façon, il y a de bonnes chance que ça soit une arnaque.

Si tout le monde fait cela, l'activité sera moins rentable pour les spammeurs, et ça aidera peut-être à réduire le volume mondial de spam.

Retour

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

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.

Retour

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 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 possesion de votre numéro de carte.

Retour

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.)

Retour

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.

Retour

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 pornogaphie infantile.

Retour

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.

Retour

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...).

Retour

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, Pixia, ArtWeaver, ArtRage.*
- Microsoft Office ? Prenez *OpenOffice*
- 3D Studio Max ? Prenez *Blender*
- Adobe Illustrator, CorelDraw, FreeHand ? Prenez *Inkscape*, *Sodipodi*.
- Visio ? Prenez *Dia*.
- Publisher, Quark XPress ? Prenez *Scribus*.
- Norton Antivirus ? Prenez *Avast Home Edition*
- Norton Internet Security ? Prenez *ZoneAlarm*
- ACDSee ? Prenez *XNView*
- SoundForge, GoldenWave, CoolEdit ? Prenez *Audacity.*
- Teleport Pro ? Prenez *HTTrack*
- CloneCD ? Prenez *BurnAtOnce*
- Nero ? Prenez *CD Burner XP Pro*
- WinZip ? Prenez *IZarc* ou *7-Zip*.
- PC Anywhere ? Prenez *VNC*
- FlashGet, GetRight ? Prenez *Free Download Manager*
- etc.

Retour

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 (comme l'excellent petit logiciel *SyncBack*, gratuit et efficace).

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 (textes, photos, musiques...).

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.

Retour

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.

Retour

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 résoud pas tous les problèmes, mais cela réduit notablement les risques (notamment si votre firewall personnel (ZoneAlarm ou autre) a un disfonctionnement).

Par exemple, voici un guide pour active le mode routeur de la Freebox.

Pour les box des autres fournisseurs d'accès, consultez la documentation fournie avec.

Retour

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.

Retour

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 ou WPA2 (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.

Retour

Notes

1. La sécurité à 100% *n'existe pas* . Je ne vous garantie 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.

Liens

- Je vous recommande l'*excellent* site http://assiste.com
  Ce site contient une somme de travail impressionnante sur la sécurité informatique et vous y trouverez de très nombreux conseils, réponses à vos questions, liens et logiciels utiles.
- Un très bon site avec un incroyable travail sur la sécurité sous Windows: http://www.malekal.com/
- Un autre site plein de bons conseils et de guides: http://gerardmelone.free.fr/IT/IT.html
- Les recommandations «safe-hex» de Claymania: http://www.claymania.com/safe-hex-fr.html
- L'ABC de la sécurité: http://abcdelasecurite.free.fr
- La FAQ (Questions fréquemment posées) du forum fr.comp.securite.virus : http://www.lacave.net/~jokeuse/usenet/faq-fcsv.html
- Un document similaire en anglais du CERT: http://www.cert.org/tech_tips/home_networks.html
- Si cela ne suffit pas, voici des liens vers divers forums où venir poser vos questions.
  Merci de faire d'abord une recherche sur Google et sur ces forums *avant* de poser votre question . Il est très probable que quelqu'un a déjà eu le même problème et que la solution a déjà été donnée.
  - http://www.commentcamarche.net/forum/
  - http://forum.hardware.fr
  - http://forum.clubic.com
  - http://forum.telecharger.com
  - http://www.forumschoixpc.com
  - http://forums.zdnet.fr/

Historique des mises à jour de ce document

- **19 mars 2004:**
  - première version.
- **18 avril 2004:**
  - Merci aux internautes pour leur *très* chaleureux accueil de ce document, pour leurs témoignagnes de sympathie, et pour toutes les corrections, commentaires, suggestions et critiques.
  - Nombreuses fautes de frappe/orthographe/grammaire corrigées.
  - Point q014c ajouté (*Je sais utiliser mon antivirus et le configurer. J'en ai lu la documentation.*)
  - Point q017b ajouté (*J'ai compris que les adresses d'expéditeur d'email peuvent être totalement falsifiées.*)
  - Point q019b ajouté (*Je sais configurer Internet Explorer et Outlook Express pour désactiver ActiveX et l'active scripting (VBScript, Javascript, WSH...)*)
  - Point q048b ajouté (*Je sais désactiver la restauration système en cas de problème.*)
  - *Spamgourmet* permet maintenant également d'envoyer des mails.
  - Liens supplémentaires: *Safehex* chez Claymania, et la FAQ de fr.comp.securite.virus.
- **27 mai 2004:**
  - Point q012b ajouté (*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.*)
  - Point q032b ajouté (*Je choisis de bons mots de passe.*)
  - Ajout d'un lien vers l'excellent site de Gérard Melone.
  - Ajout de liens vers les disquettes de boot sur severinterrier.free.fr.
  - Ajout d'un lien vers l'ABC de la sécurité.
- **1er novembre 2004:**
  - *StarDownloader* et *NetTransport* remplacés par *Free Download Manager*.
- **25 décembre 2004:**
  - Ajout de la recommandation de ne plus utiliser Internet Explorer (J'aurais dû mettre cela bien plus tôt).
- **21 février 2005:**
  - Ajout du lient vers morceauxchoisis.free.fr
- **26 septembre 2005:**
  - Mise à jour de la liste des antivirus en ligne (r048).
  - Suppression de la suggestion d'utiliser *Kerio Personal Firewall*, car l'éditeur a annoncé la mort de ce logiciel.
- **30 octobre 2005:**
  - Point q063b ajouté (*Si j'ai une "box" (Freebox, LiveBox, C-Box, AOLBox...) et que l'option "Routeur" est disponible, je l'ai activée.*).
  - Point sur le WiFi (q065) complété (WEP/WPA).
  - Microsoft a racheté RAV Antivirus: l'antivirus n'est donc plus disponible en ligne. :-(
- **11 septembre 2006:**
  - Correction URL admin Freebox dans question r063b.
  - Correction URL téléchargement mise à jour McAfee (sdatXXXX.exe) dans question r025.
- **15 novembre 2006:**
  - Mise à jour des liens des antivirus en ligne. Ajout indication où cliquer. Ajout McAfee en ligne. (Dans question r048.)
- **5 février 2007:**
  - Ajout de l'antivirus en ligne F-Secure (Dans question r048).
- **15 février 2007:**
  - Ajout des antivirus en ligne *Microsoft Live OneCare* et *CA Web eTrust* (Dans question r048).
- **22 avril 2007:**
  - Secusys.com retiré car le site a fermé (Dans question r036).
- **4 juillet 2007:**
  - Mise à jour du lien vers le site de Gérard Melone.
- **26 février 2007:**
  - Ajout de nanoscan à la liste des antivirus en ligne et petites mises à jour (Dans question r048).
- **8 mai 2008**
  - Refonte du document.
  - Mise sous contrat CreativeCommons by.
  - Question r034 reformulée (serveurs --> tous les logiciels). Ajout de logiciels pour aider à mettre à jour les logiciels.
  - Question r048: Mise à jour de la liste des antivirus en ligne.
  - Diverses modifications mineures.
- **21 mai 2008**
  - Dans WindowsUpdate: plus de mises à jour de sécurité de Windows XP après le 30 juin 2008.
- **5 juin 2008**
  - Ajout lien vers le guide pour mettre à jour Spybot S&D.
- **11 juin 2008**
  - Ajout lien vers grande liste d'antivirus en ligne dans la question r048 (merci espion3004).
- **18 juin 2008**
  - Ajout d'un lien vers l'histoire de l'internaute accusé de pédophilie.
- **2 juillet 2008**
  - Modification de la date de fin de support des mises à jour pour Windows XP (avril 2014) (dans la section WindowsUpdate)
  - Modification URL Firefox pour pointer vers la page en français.
- **28 janvier 2009**
  - Ajout de la recommandation de l'extension WOT pour Firefox qui permet d'éviter les sites douteux, spywares, faux antivirus, faux antispywares...
- **7 février 2009**
  - Antivir est aussi désormais en français.

- **13 mars 2009**
  - Ajout de WOT (Web Of Trust) dans les recommandations.
- **31 mars 2009**
  - Mise à jour de la liste des antivirus en ligne (r048) et ajout des scanner de fichier individuel multi-antivirus.
- **21 septembre 2009**
  - Mise à jour mineures sur les antivirus en ligne.
  - Ajout du lien vers le site de malekal.
- **16 juin 2010**
  - TrendMicro n'est plus un scanner en ligne (r048), mais à télécharger.
  - Ajout de plusieurs autres antivirus à télécharger (Dr.Web CureIt, McAfee Stinger, PrevX CSI Free).
  - Ajout du paragraphe "*Pensez également à mettre vos logiciels à jour*", mise à jour Flash et *Secunia PSI* dans section "WindowsUpdate".
  - Dans la section "WindowsUpdate", ajout des notes concernant les SP1/SP2/SP3 de Windows XP (ainsi qu'un lien pour télécharger le SP3).
  - Correction du lien "Avast" édition gratuite dans section "Antivirus".
  - Ajout de *MalwareBytes* dans la section "Antispyware".
  - Ajout de *Google Chrome* dans la section *Firefox*.
- **20 août 2010**
  - Correction des liens et mentions dans les antivirus en ligne.
  - L'antivirus *Command On Demand* n'existe plus. Je l'ai retiré de la liste des antivirus en ligne.
- **30 mars 2011**
  - Liens corrigés pour mettre à jour son antivirus sans connexion internet (r025).

-- fin du document --