

« Lutter contre les virus informatiques »»

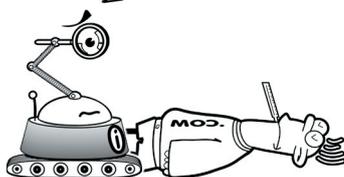
Vous avez un accès à Internet, vous utilisez le courrier électronique ou les disquettes de votre petit frère, alors vous avez forcément été confronté à un virus, peut-être même sans vous en apercevoir. Rassurez-vous, on s'en débarrasse plus facilement que de la grippe.

▷▷ Détecter les virus

Se faire infecter par un virus n'est pas catastrophique, même s'ils peuvent perturber sérieusement le fonctionnement normal de votre ordinateur (messages incongrus, exécution de tâches non sollicitées, perturbation du système et des logiciels installés, pertes de données...) voire l'endommager physiquement en s'attaquant à votre disque dur. Pour vous contaminer, les virus utilisent les moyens de communication des données : le courrier électronique, les disquettes et les CD, mais aussi le téléchargement. En fait, dès que vous copiez des données sur votre disque dur, vous prenez un risque. Sauf si vous les contrôlez à l'aide d'un antivirus.

Com, je t'ai déjà dit que les virus n'infectaient que les machines !!!

Une fois enregistrés sur votre disque dur, la majorité des virus ne deviennent nuisibles que si vous lancez le programme ou si vous ouvrez le fichier dans lequel ils résident. Installer un antivirus permet de les détecter et, dans la majorité des cas, de les éradiquer sans effort.



Se protéger

Lutter contre les virus informatiques

Eliminer les virus

Un antivirus ne peut pas détruire un programme malicieux qu'il n'est pas capable d'identifier, comme si vous aviez été immunisé contre la grippe et qu'une souche plus virulente apparaissait : le vaccin serait alors inefficace. Une piqûre de rappel s'impose. En informatique, une visite mensuelle sur le site de l'éditeur pour mettre à jour votre antivirus augmentera son efficacité : il reconnaîtra tous les virus apparus depuis la dernière mise à jour. Dans le pire des cas, vous devrez patienter quelques jours, le temps que des ingénieurs trouvent un antidote. Malheureusement, ce n'est pas aussi simple en médecine...

Que faire si vous êtes infecté par un virus ?

Il faut :

- Eviter d'utiliser votre ordinateur. Ne plus poster de messages, ne plus vous connecter à d'autres machines, ne plus enregistrer de disquettes ni de CD...
- Prévenir les personnes que vous auriez pu contaminer depuis une autre machine ou par téléphone.
- Tenter d'identifier la source d'origine du virus (nouvelle disquette, derniers messages...), tout en sachant qu'il existe des virus dormants, programmés pour se déclarer à une date définie.
- Si le virus est nouveau, consulter les sites spécialisés, notamment celui de Microsoft puisque la plupart des virus portent leurs attaques sur ses produits les plus utilisés (Outlook, Internet Explorer). *A contrario*, les utilisateurs de Mac, de logiciels libres sont moins exposés aux contaminations. N'hésitez pas à demander à une personne plus compétente si vous ne vous en sortez pas.

On trouve deux types d'antivirus : les payants, disponibles sous licences commerciales et les gratuits, la plupart du temps réservés à une utilisation privée et non commerciale. Pour une version propriétaire, comptez moins de 60 euros, avec des mises à jour gratuites durant la première année. Ensuite, vous devrez vous acquitter annuellement d'un droit d'abonnement pour bénéficier de ce service (moins de 10 euros).

Parmi les antivirus qui ont la confiance des internautes, on peut citer les logiciels gratuits tels que avast ! Virus Cleaner, BitDefender Free Edition, Clean Sasser (créé spécialement pour exterminer le virus Sasser), AVG Free Edition...



Se protéger

Lutter contre les virus informatiques

Les fichiers dont il faut se méfier

Si jamais vous recevez un courriel d'une de vos connaissances et que le message est rédigé en anglais, langue de prédilection des propagateurs de virus, **méfiez-vous** ! Enregistrez ce fichier sur le disque dur sans l'ouvrir. Et si l'extension du fichier est contenu dans cette liste, vérifiez-le avec un antivirus à jour.

**.mdb .mde .bat .pif .com .xls .xlt .js
.ppt .pps .vbs .exe .scr .doc .dot .reg**

Rappelez-vous aussi que les virus sont rusés et que pour vous tromper, certains fichiers arrivent avec des extensions doubles. Par exemple, achillezavatta.jpg.bat vous apparaîtra sous la forme achillezavatta.jpg sous Outlook si Windows est paramétré pour cacher les extensions. Ce n'est pas une image au format .jpg, mais bien un programme malicieux.

Soyez aussi prudent si vous recevez ou téléchargez des données incluses dans des fichiers compressés (zip...).

Savoir plus

Le ver, un membre éminent de la famille des virus

Le ver est un programme capable de s'auto-reproduire et de se déplacer à travers un réseau. Il peut propager une version fonctionnelle et complète de lui-même vers d'autres ordinateurs. Il fonctionne de manière indépendante et n'a pas besoin d'un support physique ou logique (disque dur, programme hôte, fichier joint...) pour se diffuser. C'est ce que l'on appelle un virus réseau. Son but est de se répandre d'ordinateur en ordinateur via les connexions réseau en se reproduisant à l'infini. A cause de leur vitesse de reproduction, ils ont pour principal effet de saturer la bande passante.

Un antivirus à jour permet de se débarrasser de quasiment tous les vers.



Prévenir, c'est guérir

Plutôt que de traquer le virus dans toutes les parties de votre disque, évitez-les. Cette liste de conseils devrait vous y aider.

- Avant d'ouvrir une pièce jointe contenant un fichier exécutable (se terminant par .exe, .com, .sys, .pif...), scannez-la avec votre antivirus. D'une manière générale, méfiez-vous des courriels de grande taille dont vous ne connaissez pas la provenance.
- Analyser vos disquettes, CD et DVD avant de les lire.
- Paramétrez Windows pour que le logiciel de messagerie que vous utilisez affiche systématiquement les extensions de fichiers.

Se protéger

Lutter contre les virus informatiques

- . Enregistrez et testez tous les fichiers que vous téléchargez sur Internet, surtout si vous faites du « peer to peer » ou que les données ne proviennent pas d'un site « institutionnel », sûr. Même si les antivirus vérifient toutes nouvelles données sensibles avant que vous ne les lanciez, mieux vaut ne pas « exécuter » directement le fichier mais l'enregistrer sur le disque dur (option « enregistrement » plutôt que « ouvrir avec... »). Comme pour une pièce jointe, vous pourrez analyser le fichier avec votre antivirus avant de l'exécuter.
- . Créez un Recue Disk afin de pouvoir analyser son disque dur et éliminer le virus sous MS-DOS lorsque l'ordinateur est contaminé et que vous n'arrivez plus à retourner sous Windows.
- . Partitionnez votre disque dur, séparez les données des applications pour éviter de contaminer la totalité de votre disque, l'idéal étant d'avoir un deuxième disque dur.

De toute façon, ce n'est pas la peine d'en faire une jaunisse si jamais votre machine est « vérolée ». Le remède existe ou va être mis au point. Se débarrasser d'un virus est donc une opération plus facile qu'on le croit et suivre quelques règles de bases permet d'éviter la plupart des infections.



En résumé

Pour mettre son ordinateur et celui des autres à l'abri

Il faut :

- . Installer un antivirus, un pare-feu pour éviter une contamination ou l'invasion d'un Trojan.
- . Faire une image de votre disque dur avec un « ghost » afin d'éviter de tout réinstaller en cas de panne.
- . Sauvegarder fréquemment vos données.
- . Faire le ménage : vider la corbeille, supprimer les fichiers temporaires...
- . Défragmenter votre disque dur.
- . Faire un ScanDisk, même si l'opération est longue, tous les trois mois afin de réparer les parties (clusters) abîmées, le changer si une grande proportion de clusters sont inexploitable.
- . Surveiller le comportement de votre machine (souris qui n'obéit plus, impression non-sollicitée, ralentissement du disque dur...).
- . Vous créer une deuxième adresse mail que vous consacrerez aux usages « publics » : forums, chats, achats en ligne, lettres de diffusion...

Il ne faut pas :

- . Ouvrir ou lancer des logiciels de provenance douteuse (site warez, pirate, de pair à pair...), il est préférable les enregistrer sur le disque et les scanner avec un antivirus avant de les ouvrir.
- . Ouvrir un courriel indésirable, répondre à un mail dont l'expéditeur vous est inconnu.

Si vous n'utilisez pas votre ordinateur personnel :

- . Inspecter l'ordinateur avec un antispyware, si c'est possible.
- . Vérifier si un utilisateur de la machine peut installer un logiciel. En cas de doute, il ne faut pas vous connecter à des sites sécurisés, comme celui de votre banque.