

Cours « Sécurité »

1 – Notion de sûreté de fonctionnement

Il y a deux notions abordées dans ce cours : la sécurité et la sûreté de fonctionnement.

- La sécurité informatique vise à se protéger des attaques délibérées d'individus malveillants.
- La sûreté de fonctionnement vise à protéger votre système d'une défaillance technique.

La défaillance technique est une réelle menace pour un ordinateur. Un disque dur, malgré une durée de vie de plusieurs années, n'est pas infaillible et peut être détérioré à la suite d'un **pic de tension** dans le réseau électrique ou d'une **simple coupure de courant**, notamment par temps orageux.

La **poussière** est également l'ennemi de votre ordinateur : pensez à passer un coup d'aspirateur de temps en temps autour de votre unité centrale ! Cela évitera que la poussière ne rentre dans votre ordinateur et ne crée de courts-circuits.

Les **modems** (à travers les lignes téléphoniques) sont également sensibles aux surtensions : par temps orageux ou lors d'un départ de plusieurs jours, pensez à débrancher les prises électriques et les lignes téléphoniques reliées à votre ordinateur !

Les supports de stockages peuvent aussi être endommagés :

- Les disquettes (méfiez-vous des sauvegardes sur disquettes)
- Les CD-ROMs (vérifiez après la gravure que les informations sont bien inscrites)
- Les disques durs (ça arrive rarement, mais ça arrive)

2 – Sauvegarder vos données régulièrement !

Le risque pour la majeure partie des utilisateurs est bien sûr la perte des données, des documents qu'il a fallu des jours, voire des mois à informatiser. Par conséquent, la première chose à faire est de sauvegarder régulièrement ces données. Si vous disposez d'un graveur ou d'un lecteur Zip, il vous sera facile d'effectuer ces sauvegardes régulièrement, de préférence, bien entendu, lorsqu'une tâche importante vient d'être achevée.

Pour des données très sensibles, il est possible de prendre une précaution supplémentaire en stockant ces sauvegardes dans un lieu différent de celui où se situe le système, de façon à pallier la perte du support de sauvegarde en cas d'incendie par exemple.

Ces différentes sauvegardes pourront toutes être conservées si elles sont inscrites sur un CD-R (*Recordable*), mais l'utilisation du CD-RW (*Rewritable*), qui permet de n'employer qu'un seul disque de sauvegarde, est ce qui revient moins cher à long terme. Il faut dans ce cas disposer d'un graveur capable de gérer les disques réinscriptibles, ce qui est le cas de tous les graveurs du marché actuellement.

3 – Les virus

Un ver (en anglais worm) est un agent autonome capable de se propager à l'intérieur de la mémoire d'un ordinateur, passant d'un système à l'autre grâce au réseau informatique. Ce type de programme est différent d'un virus. Pour commencer, un ver n'attaque pas les données personnelles de l'utilisateur. Il se contente simplement de se reproduire par le biais d'Internet jusqu'à infester un maximum de machines.

Par contre, un virus est un programme destructeur, dont le but est de se déplacer de machine en machine pour propager son action. Il s'attache à d'autres fichiers, souvent des exécutables (.com ou .exe dans le monde Windows), pour pouvoir circuler sur le réseau. Avant le développement d'Internet, les virus se propageaient presque uniquement grâce à l'échange de disquettes. En contrôlant leur emploi, on pouvait alors se protéger efficacement. Aujourd'hui, les virus se servent principalement des courriers électroniques et circulent donc par Internet. Les documents Microsoft Office, notamment, grâce aux macros qu'ils contiennent, peuvent abriter des virus très virulents.

Une des méthodes les plus efficaces contre les virus est (mis à part l'antivirus) de ne jamais ouvrir un fichier dont on ne connaît ni l'expéditeur ni le contenu. Les virus utilisent en effet les carnets d'adresses des victimes pour propager leurs actions dévastatrices. Vous croyez alors recevoir un message contenant un fichier envoyé par un ami, et votre vigilance est largement diminuée.

Pour se protéger contre les virus, la première précaution à prendre est de tester systématiquement les disquettes étrangères à votre ordinateur avec un antivirus. Cependant, le courrier électronique représente également une forte menace. Il est donc indispensable :

- De **ne jamais ouvrir un fichier attaché** venant d'un utilisateur inconnu.
- De **ne jamais ouvrir un fichier attaché exécutable** (.com, .exe, .pif...), **même si vous connaissez celui qui vous l'envoie**. Avant d'ouvrir un tel fichier, assurez-vous toujours que votre correspondant vous l'a envoyé volontairement.
- De toujours **désactiver les macros Word ou Excel** des fichiers attachés, même si elles viennent d'un utilisateur connu. Celles-ci peuvent être de véritables nids de virus.
- D'utiliser un anti-virus **régulièrement mis à jour**

Remarque : Un virus peut-il détruire mon ordinateur ?

Tout dépend du sens que vous donnez au mot détruire : un ordinateur dont le disque dur est vidé ne sert en effet plus à grand-chose, mais il est possible de le remettre en état, au prix d'une réinstallation logicielle du système d'exploitation et de vos applications.

En revanche, contrairement à ce que certaines rumeurs peuvent colporter, **un virus ne peut en aucun cas détruire matériellement votre ordinateur.**

4 – Comment se protéger des virus ?

Il existe un programme spécialement conçu pour se protéger contre les virus : l'antivirus.

De nombreux logiciels de ce type sont disponibles sur le marché, à tous les prix et avec des performances très diverses. Ce dernier devra être mis à jour régulièrement : tous les vendeurs d'antivirus mettent à disposition de leurs clients les mises à jour de leur logiciel sur leur site internet.

Remarque : Les antivirus détectent-ils tous les virus ?

Les antivirus doivent être fréquemment mis à jour pour être efficaces : de nouveaux virus émergent tous les jours, plus ou moins virulents, et des ajouts de programmes (ou "patches") permettent de les contrer. Ainsi, lorsque votre machine a un comportement visiblement différent de celui auquel vous êtes habitué, votre premier réflexe doit être de scanner l'ensemble des disques durs ainsi que la mémoire vive pour détecter un éventuel virus.

Si votre antivirus ne trouve pas de virus, deux cas sont possibles : le premier c'est simplement que ce virus n'a pas encore été répertorié par l'antivirus. Cette possibilité est tout à fait envisageable, mais sachez qu'il ne faut généralement qu'un ou deux jours aux entreprises commercialisant les antivirus pour répertorier un virus dans leurs bases.

Ainsi, par expérience, si votre antivirus est à jour, c'est généralement la deuxième hypothèse qu'il faudra privilégier : celle d'une défaillance de votre système d'exploitation suite à une mauvaise configuration ou à une erreur de manipulation.

5 – Antivirus

Le logiciel le plus connu (mais payant) : Norton Antivirus.

Le logiciel gratuit le plus utilisé : Avast! Disponible sur le site, <http://telecharger.01net.com>

Enfin, un antivirus gratuit en ligne : <http://www.secuser.com/antivirus/index.htm>

La majorité des anti-virus se mettent automatiquement à jour.

6 – Windows Update

Windows propose une fonctionnalité appelée **Windows Update** qui permet de maintenir le système à jour et de corriger certaines erreurs : il télécharge automatiquement les mises à jour lorsque vous êtes connectés et il est alors recommandé d'accepter les modifications proposées par Windows.