

La sécurité sur Internet

L'usage croissant d'Internet a engendré un développement exponentiel des «attaques» extérieures sur les systèmes informatiques.

De nature variée, ces «agressions» peuvent engendrer des pertes de données ou des blocages conséquents sur les ordinateurs touchés.

La **menace** (virus, spam, hoax,...) représente le type d'intrusion susceptible de nuire à la structure visée.

La **vulnérabilité** correspond au degré d'exposition d'un système informatique face à une menace précise dans un contexte particulier.

Enfin la **contre-mesure** est l'ensemble des actions mises en œuvre en prévention de la menace.



Les virus

Les virus sont introduits sur un ordinateur par un lecteur externe (disquette, clé USB, zip, cd-rom, dvd-rom, etc.) ou par messagerie. Ils se reproduisent en infectant les logiciels et/ou leurs données.

Chaque virus est identifié par une **signature virale**. Les antivirus s'appuient sur cet élément pour les détecter. Cette méthode n'est fiable que si l'antivirus possède une **base virale à jour**, c'est-à-dire comportant les signatures de tous les virus connus.

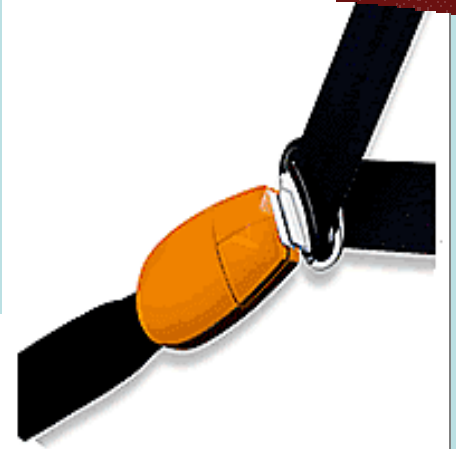
Les antivirus

Un antivirus est un programme capable de **détecter la présence de virus** sur un ordinateur et de le désinfecter (**détruire** le virus ou le mettre en **quarantaine**) dans la mesure du possible.

Afin de préserver l'ordinateur, il est indispensable d'effectuer une mise à jour régulière de la **base virale** (liste des virus reconnus). Cette opération s'effectue de deux façons :

- se connecter au site web du fournisseur de l'antivirus et télécharger la dernière version de la base virale,
- configurer soi-même l'antivirus pour qu'il fasse cette mise à jour automatiquement et régulièrement.

Régulièrement, il est nécessaire de lancer manuellement une analyse complète de l'ordinateur par l'antivirus pour s'assurer qu'aucun virus ne soit entré entre temps.



La sécurité sur Internet

Les firewall (pare-feu)

Chaque ordinateur connecté à Internet est susceptible d'être victime d'une menace envoyée par un « pirate » informatique. Celui-ci cherche une faille de sécurité pour accéder aux données de l'ordinateur et les modifier.

Cette menace augmente si la machine est allumée et connectée en permanence à Internet.

Un outil « pare-feu » sert à protéger un ordinateur ou un réseau d'ordinateurs des intrusions extérieures. Il permet en effet de repérer et d'empêcher l'ouverture non autorisées d'autrui à se connecter à Internet.

Le pare-feu se présente de deux manières :

- un logiciel pour chaque ordinateur relié à Internet. Cette solution est généralement appliquée dans les petites structures.
- un boîtier qui protège tous les ordinateurs de la structure. Il est positionné entre le réseau d'ordinateurs et l'entrée d'Internet dans le réseau. Cette solution est appliquée pour les réseaux informatiques de plus grande taille.

Le spam

Un « spam » désigne l'envoi massif de courrier électronique, ayant un caractère souvent publicitaire, à des destinataires ne l'ayant pas sollicité. Les adresses utilisées par un spam sont généralement récupérées sur Internet.

Pour l'internaute, les inconvénients majeurs du spam sont :

- L'espace occupé dans les messageries électroniques par leur nombre important,
- La difficile consultation des messages destinés en propre qui sont noyés au milieu de spams,
- Le risque de suppression erronée ou de non lecture de messages importants,
- La perte de temps occasionnée par leur tri et leur suppression,
- Le caractère violent ou dégradant de certains spams,
- L'encombrement du trafic sur Internet,
- La présence de hoax (type de spam). C'est un message dont le contenu, se présentant comme véridique, est faux. Ces messages vous proposent de les transférer à plusieurs destinataires.

Le site <http://www.hoaxbuster.com> permet d'identifier ce type de message indésirable.

Combattre le spam :

On distingue généralement deux familles de logiciels anti-spam.

* Les dispositifs côté utilisateur

Il s'agit généralement de logiciels dotés de filtres qui identifient les messages, sur la base de règles prédéfinies ou d'un apprentissage automatique de l'anti-spam.

Cet outil a l'avantage d'être intégré à la plupart des logiciels de messagerie actuels, donc gratuit et son installation est aisée.

* Les dispositifs côté serveur

Ils permettent de filtrer le courrier avant son arrivée sur la messagerie du destinataire.

Son efficacité repose sur une intervention en amont du réseau, c'est-à-dire, avant son arrivée sur le serveur de messagerie, et évite ainsi l'engorgement des réseaux et des boîtes aux lettres.

Plus efficace que les dispositifs côté utilisateur, cette solution est cependant plus coûteuse et nécessite l'intervention d'une personne qualifiée.

Eviter le spam

Pour se préserver des spams, il est nécessaire de limiter au maximum la diffusion de son adresse électronique sur Internet. A ce titre, il est donc important de :

- Détruire les messages invitant l'utilisateur à transmettre le courrier au maximum de contacts possible.(chaîne).
- Eviter au maximum de publier son adresse électronique sur des forums ou des sites Internet
- Créer une ou plusieurs « adresses jetables » servant uniquement à s'inscrire ou s'identifier sur les sites jugés peu fiables quand au respect de la confidentialité de son adresse e-mail.