

# Se protéger Lutter contre les espioniciels

**V**otre ordinateur a un comportement anormal : des fenêtres publicitaires s'ouvrent à tort et à travers lorsque vous surfez sur Internet, l'adresse de votre page de démarrage a changé sans votre accord... Cela signifie que vous avez été infecté par un espioniciel. Rien de grave, à condition de vous en débarrasser.

## « A l'insu de votre plein gré »

Un espioniciel, plus connu sous son nom anglais de *spyware*, est un programme chargé de recueillir des informations sur l'utilisateur de la machine sur lequel il est installé. Son but est de récolter et de transmettre ces informations, c'est pourquoi on l'appelle parfois mouchard.

En général, un espioniciel s'installe en même temps qu'un autre logiciel, le plus souvent des gratuits (freewares) ou des partagiciels (sharewares). Ainsi, l'auteur rentabilise son programme grâce à la vente d'informations statistiques. On peut donc parler d'un véritable modèle économique où la gratuité du logiciel est obtenue contre la cession de données personnelles. D'autant que les espioniciels ne sont pas illégaux. Souvent, la licence d'utilisation qui accompagne le logiciel précise qu'un tel programme va être installé. Mais qui lit une licence d'utilisation en entier ? Si vous faites encore cet effort, méfiez-vous des formules du type « peut contenir un logiciel vous avertissant occasionnellement d'informations importantes », en anglais « *may include software that will occasionally notify you of important news* ».

## Savoir +

### Ce que l'espioniciel peut savoir

#### Un espioniciel peut savoir :

- les sites internet que vous visitez
- les mots-clés que vous saisissez dans les moteurs de recherche
- les achats que vous réalisez sur Internet
- les informations de paiement bancaire (numéro de CB, Visa...) pour les plus sournois
- et d'une manière générale, tout ce qu'il y a dans votre machine



# Se Lutter contre les **espiogiciels** >>>

Comme pour les virus, quelques **précautions** simples permettent de les éviter. Et même en cas d'infection, la situation n'est pas dramatique. Des programmes spécialisés les éliminent, comme le font les antivirus avec les codes malicieux.

Comme tout bon espion, le *spyware* est difficile à détecter. La meilleure façon de **s'en protéger**, c'est encore de ne pas installer de logiciels dont la provenance n'est pas sûre. En particulier, les gratuits, les partagiciels et les logiciels d'échange de fichiers de pair à pair. D'autant plus que la désinstallation d'un logiciel ne supprime que rarement l'espiogiciel qui l'accompagne.

Si la première parade consiste à ne pas installer n'importe quoi, a fortiori si vous êtes un adepte des logiciels de pair à pair ou des sites peu recommandables, elle ne suffit pas pour assurer une protection sans faille.

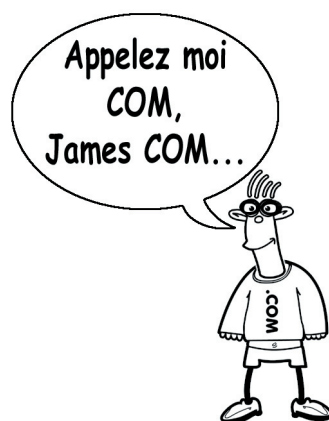
Il faut la **combiner à une autre méthode** qui consiste à mettre à jour votre navigateur et à éviter l'exécution de scripts Active X avec Internet Explorer. Par défaut, celui-ci est paramétré pour ne les exécuter qu'après confirmation. Pour le vérifier, cliquez sur le menu Outils/Options d'Internet Explorer. Dans l'onglet Sécurité de la fenêtre Options Internet, vérifiez que le niveau de sécurité Moyen est associé à la zone sécurité Internet. Seuls les contrôles Active X dotés d'un certificat s'exécutent automatiquement. Ce qui devrait vous éviter un certain nombre de désagréments. Si vous utilisez le navigateur Firefox, notez que le succès aidant, il risque de devenir la prochaine cible des *spywares*.

## Savoir +

### Comment l'espiogiciel nuit à votre machine ?

Outre le désagrément causé par le fait de se savoir épié, les espiogiciels nuisent aussi à l'ordinateur :

- . en consommant de la mémoire vive
- . en utilisant de l'espace disque
- . en sollicitant le processeur
- . en empêchant le fonctionnement normal de certaines applications (plantage machine systématique)
- . en ouvrant des écrans publicitaires ciblés en fonction de l'information collectée lorsque vous surfez sur Internet
- . en utilisant de la bande passante



# Se Lutter contre les **espioniciels** >>>

protéger

Pour vous débarrasser des espioniciels, il faut utiliser un **antispyware**. Les trois plus connus sont :

Spybot Search & Destroy que vous pouvez télécharger gratuitement :

<http://www.spybot.info/fr/mirrors/index.html>

Ad-Aware que vous pouvez télécharger gratuitement :

<http://lavasoft.element5.com/default.shtml.fr>

[http://www.download.com/Ad-Aware-SE-Personal-Edition/3000-8022\\_4-10045910.html?part=dl-ad-aware&subj=dl&tag=top5](http://www.download.com/Ad-Aware-SE-Personal-Edition/3000-8022_4-10045910.html?part=dl-ad-aware&subj=dl&tag=top5)

Microsoft Antispyware que vous téléchargez gratuitement en version bêta :

<http://www.zdnet.fr/telecharger/windows/fiche/0,39021313,39105760s,00.htm>

Selon les journaux et les sites spécialisés, ce sont les trois meilleurs logiciels pour lutter contre les espioniciels. Néanmoins, ces outils ont un inconvénient majeur : chaque logiciel ne reconnaît pas les mêmes spywares. Ainsi, un espioniciel détecté par un programme ne l'est pas forcément par un autre. Une bonne solution consiste à les combiner. Comme pour les antivirus, une mise à jour régulière est nécessaire pour qu'il reste efficace.

Pour **neutraliser** les logiciels espions, vous pouvez aussi installer un pare-feu qui les empêchera de se connecter à Internet et de transmettre les informations collectées sur votre machine. Le *spyware* sera toujours installé sur votre machine, mais son action sera enrayée.

Rassurez-vous, si un *spyware* peut être très nuisible, il suffit généralement d'une dizaine de minutes pour l'éradiquer ou, au moins, le neutraliser.

## Savoir +

### Le publiciel, un espioniciel spécialisé

Peu virulent, mais très fréquent, le publiciel est un espioniciel qui affiche des publicités ciblées, sous la forme de bannières ou de fenêtres «pop-up». En fonction des informations récupérées sur votre ordinateur (sites visités, achats effectués en ligne...), ils affichent la réclame censée vous intéresser. Ils effectuent donc un véritable profil de l'utilisateur. La conséquence principale d'une telle infection est la gêne occasionnée : les pages sont plus longues à télécharger et vous ne pouvez plus surfer sans être renvoyé vers des «pop-up» publicitaires. En anglais, on le nomme *adware*, contraction des mots *advertising* (publicité) et *software* (logiciel).

### Les plus perfides

Il existe d'autres spécialistes de l'espionnage. Les internautes qui utilisent une connexion bas débit via une ligne téléphonique classique doivent se méfier plus particulièrement des *composeurs* (*dialers* dans la langue de Shakespeare) qui appellent – à l'insu de l'utilisateur – un numéro surtaxé. Méfiez-vous aussi des *keyloggers* qui peuvent transmettre à un tiers toutes les frappes clavier, votre numéro de carte de crédit par exemple.

