

## Résumé

Les virus et les vers (veuillez également consulter la fiche Vers/Virus) ont pour vocation d'infecter une machine, comme un ordinateur ou un serveur, à l'insu des utilisateurs pour y exécuter un logiciel illicite, et se propager d'une machine à une autre. Les virus et les vers peuvent concerner toute personne, lors des échanges d'informations par courrier électronique, par

transferts via des médias ou en téléchargeant des logiciels, documents ou tout autre type de fichiers depuis Internet. Afin de se protéger efficacement contre cette menace générique constante, il convient d'installer des mécanismes de sécurité particuliers, à savoir les anti-virus qui sont décrits dans ce document.

## Table des matières

- 1 C'est quoi ? →
- 2 Qui est concerné ? →
- 3 Comment cela fonctionne-t-il ? →
- 4 Pourquoi se protéger ? →
- 5 Comment se protéger ? →



### 1 C'est quoi ?

Un anti-virus est un logiciel ayant pour objectif principal de protéger une machine contre différents types d'infections informatiques tel que des virus.

Cependant, des différences peuvent exister entre ces types de logiciels. Elles se situent principalement dans le nombre de fonctionnalités, leur mise en place ainsi que les méthodes utilisées pour la détection d'anomalies.

### 2 Qui est concerné ?

Tous les citoyens, PME et administrations confondus, échangeant des informations par courrier électronique, ou par transferts via des médias tels que disquettes, CD-ROMs, memory sticks, mais également en téléchargeant des logiciels, documents et tout autre type de fichiers depuis Internet.

### 3 Comment cela fonctionne-t-il ?

Afin de protéger une machine, les logiciels anti-virus utilisent plusieurs techniques à savoir :

- Analyse en temps réel du contenu des opérations sur la machine tel que des ouvertures/fermetures de fichiers, des lancements de logiciels et tout type de téléchargements effectués sur la machine depuis Internet ou un autre réseau.
- Balayage des disques et autres périphériques de stockage et de la configuration système de la machine à des intervalles définis préalablement.
- Analyse du contenu ainsi que des volumes de courriers électroniques entrants et sortants afin de protéger contre des virus qui possèdent un processus opérationnel de propagation par messagerie (appelés mass-mailers).

→ suite

En cas de détection d'anomalie ou de tentative d'infection informatique, dans la majorité des cas et selon la configuration choisie par l'utilisateur, l'anti-virus affichera une alerte à l'utilisateur permettant de :

- Bloquer la tentative d'infection informatique.
- Réparer le contenu infecté ou malicieux en effaçant toute trace du virus.

- Supprimer définitivement le contenu infecté.
- Mise sous quarantaine du contenu infecté ou malicieux.

Du fait de la convergence des techniques d'infection informatique, certains constructeurs de logiciels intègrent également dans leur solution d'anti-virus des fonctionnalités de firewall.

## 4 Pourquoi se protéger ?

L'utilisation d'un logiciel anti-virus permet de contrer les menaces suivantes :

**⚠ Virus**

**⚠ Chevaux de Troie**

(Veuillez également consulter le document Cheval de Troie)

**⚠ Vers**

Si l'anti-virus dispose également de fonctionnalités de firewall (veuillez également consulter le document firewall).

### → EXEMPLE d'une tentative d'infection virale détectée par l'anti-virus :

Voici un exemple de simulation d'une tentative d'infection virale détectée par l'anti-virus. Cette simulation a été effectuée par l'utilisation d'un fichier test mis à disposition par l'EICAR (European Institute for Computer Antivirus Research) disponible sous [www.eicar.org](http://www.eicar.org).



## 5 Comment se protéger ?

Pour vous protéger, il suffit de télécharger un logiciel de type antivirus. Certains sont disponibles gratuitement, en version de démonstration, sur Internet.

Cependant, un anti-virus ne pourra pas remplir son objectif si les recommandations suivantes ne sont pas appliquées, voire vérifiées :

- Configurez la mise à jour régulière (si possible journalière) de la base de signatures des virus (veuillez également consulter la fiche patch).
- Évitez d'ouvrir des courriers électroniques (e-mails), logiciels, ou tout autre fichier dont le sujet ou le contenu vous semble inhabituel voire anormal.
- Balayez tous les disques et la partie système de la machine au moins une fois par semaine.
- Vérifiez le fonctionnement correct de votre système via l'utilisation des fichiers de tests mis à disposition par l'EICAR : [www.eicar.org](http://www.eicar.org)