



LES ANTIVIRUS



En naviguant sur Internet, en cliquant sur un lien ou en ouvrant la pièce jointe d'un message, en branchant une clé USB... vous pouvez être infecté par un virus informatique. Les virus sont des programmes malveillants qui cherchent à perturber le fonctionnement normal d'un appareil à l'insu de son propriétaire ou à porter atteinte à ses données: vol ou destruction d'informations, espionnage ou chantage, utilisation de sa machine pour en attaquer d'autres... Les antivirus contribuent à vous protéger contre ces menaces. **Réponses aux 10 questions les plus fréquentes sur les antivirus.**

1 QU'EST-CE QU'UN ANTIVIRUS ?

Un antivirus est un programme informatique, ou une application, qui a pour principale vocation d'identifier, de neutraliser, voire d'éliminer les virus informatiques.

2 FAUT-IL UTILISER UN ANTIVIRUS ?

La réponse est « oui ». Même si aucun antivirus ne permet une protection absolue contre les virus, ils contribuent à être protégé des principaux virus connus. L'utilisation d'un antivirus est une des principales mesures à appliquer pour assurer votre sécurité numérique (en savoir plus: [10 mesures essentielles pour assurer votre sécurité numérique](#)).

3 CERTAINS APPAREILS PEUVENT-ILS SE PASSER D'ANTIVIRUS ?

Globalement, non. Si certains systèmes sont plus vulnérables que d'autres, tous les équipements informatiques (PC, [tablettes](#), [téléphones mobiles](#), [objets connectés](#), serveurs...) peuvent être infectés par un virus et devraient donc être protégés.

4 COMMENT FONCTIONNE UN ANTIVIRUS ?

Un antivirus se greffe sur le système d'exploitation de l'appareil. Il permet de rechercher les virus dans

ce qui peut y être stocké, y entrer ou en sortir. Cela concerne leur(s) mémoire(s) ou leur(s) disque(s) dur(s), le contenu des messages (e-mail), le chargement d'une page Internet, la lecture d'un média amovible (clés USB, DVD...). Pour cela, l'antivirus s'appuie sur des « bases de signatures » qui contiennent des définitions ou empreintes de virus régulièrement actualisées, et souvent aussi sur des analyses de comportements anormaux (dites « analyses heuristiques ») qui pourraient être liés à des virus.

5 UN ANTIVIRUS PEUT-IL RALENTIR MON APPAREIL ?

Oui, car votre antivirus va analyser toutes les actions que vous réalisez sur votre appareil pour vérifier qu'elles ne causent pas une infection par un virus, ce qui prend évidemment du temps et peut donc ralentir votre utilisation. En fonction de la puissance de votre appareil, ce ralentissement peut toutefois être imperceptible. La rapidité d'analyse peut être un critère de choix de la solution antivirus qui vous convient.

COMMENT VÉRIFIER QUE SON ANTIVIRUS FONCTIONNE ?

Pour tester le fonctionnement d'un antivirus, téléchargez le fichier en cliquant sur le lien suivant : <https://secure.eicar.org/eicar.com>

Bien que ce fichier de test soit inoffensif, votre antivirus doit vous afficher une alerte. Dans le cas contraire, vérifiez que votre antivirus est bien actif et convenablement configuré (voir point 6).



EN PARTENARIAT AVEC:

MINISTÈRE DE L'INTÉRIEUR

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

**6 COMMENT BIEN UTILISER
SON ANTIVIRUS?**

Pour bien utiliser votre antivirus, il faut vous assurer qu'il est bien installé, qu'il est activé, que la protection en « temps réel » pour analyser ce qui entre et sort est bien configurée, qu'il se met à jour régulièrement de son programme et de ses signatures. Pour cela, il faut vérifier les paramètres de l'antivirus et tester son bon fonctionnement (voir encadré en page précédente). Réalisez également régulièrement une analyse approfondie (scan) de votre matériel pour vous assurer qu'aucun virus initialement inconnu ne serait venu s'y implanter entre deux mises à jour.

**7 POURQUOI FAUT-IL METTRE
À JOUR SON ANTIVIRUS?**

Des milliers de nouveaux virus sont créés chaque jour. Pour permettre aux utilisateurs d'antivirus de rester protégés face à ces nouvelles menaces, les éditeurs réalisent des mises à jour régulières des bases de signatures, de leurs méthodes de détections heuristiques et de leurs produits. Ces mises à jour peuvent être diffusées jusqu'à plusieurs fois par jour. Il est donc primordial de s'assurer de leur installation automatique dès qu'elles sont disponibles.

**8 QUE FAIRE SI MON ANTIVIRUS
DÉTECTE UN VIRUS?**

Si votre antivirus vous alerte qu'il détecte un virus, il y a généralement trois cas de figure possibles. L'antivirus vous signale :

- qu'il a supprimé le virus ;
- qu'il a mis en quarantaine un fichier suspecté de contenir un virus ;
- qu'il a détecté un virus sans parvenir à le supprimer.

Dans tous les cas, suite à une alerte d'infection virale, il est vivement conseillé de déconnecter l'appareil d'Internet et d'en faire une analyse

approfondie (scan) pour vous assurer qu'aucune trace du virus ne subsiste sur votre équipement. De même, il est fortement recommandé de ne sortir un fichier suspect de quarantaine que si vous êtes certain qu'il n'est pas infecté. Enfin, en cas d'impossibilité de supprimer un virus, une réinstallation complète de l'appareil et un changement de tous les mots de passe utilisés doivent être envisagés.

**9 QUEL EST LE MEILLEUR
ANTIVIRUS?**

Il est difficile de répondre à cette question car les performances et fonctionnalités des principaux antivirus du marché sont assez similaires et aucun ne peut se prévaloir d'apporter une protection à 100 % efficace. Leur classement de performance varie d'un test à l'autre en fonction des critères utilisés pour leur évaluation.

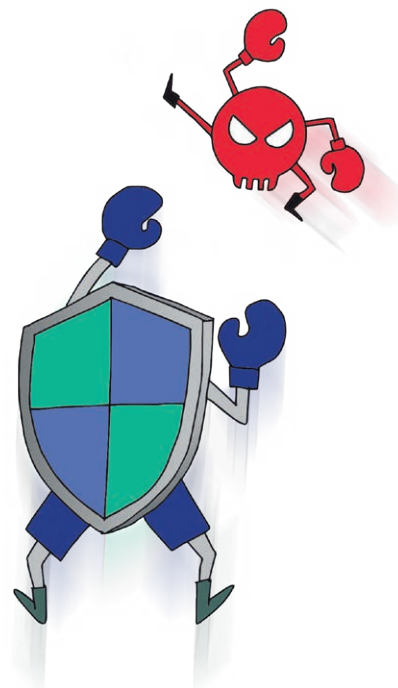
**10 ANTIVIRUS GRATUIT OU
PAYANT, LEQUEL CHOISIR?**

Aujourd'hui, les performances de protection des antivirus gratuits et payants tendent à se rapprocher sur leurs fonctionnalités de base. Les antivirus gratuits peuvent être moins gourmands en puissance machine et sont souvent plus faciles à utiliser, car ils disposent de moins de fonctionnalités que les antivirus payants. Les antivirus payants coûtent quelques dizaines d'euros par an et offrent, quant à eux, généralement plus de fonctionnalités de sécurité comme la détection de sites malveillants d'hameçonnage, la possibilité de sécuriser votre connexion à Internet avec un VPN, la fourniture d'un coffre-fort numérique pour protéger vos informations sensibles, un gestionnaire de mots de passe et même une assistance aux utilisateurs. Le choix de votre antivirus dépendra donc de

**MÉFIEZ-VOUS
DES FAUX ANTIVIRUS!**

Une fenêtre s'affiche sur votre écran vous indiquant que votre matériel est infecté et/ou vous propose d'installer un autre antivirus que le vôtre? Vous avez trouvé un site qui vous propose gratuitement un antivirus normalement payant? Fuyez, car il s'agit d'une arnaque visant à vous faire installer un faux antivirus ou un antivirus piégé justement avec un virus. Au moindre doute, redémarrez votre appareil et faites-en une analyse approfondie avec votre antivirus habituel.

vos budget, des caractéristiques et performances de votre machine et des fonctionnalités de protection que vous recherchez. N'hésitez pas à les tester et les comparer. Enfin, ne téléchargez votre antivirus que depuis le site officiel de son éditeur ou depuis les magasins logiciels officiels tels l'Apple App Store et le Google Play Store pour vos appareils mobiles (voir encadré ci-dessus).

**RETROUVEZ TOUTES NOS PUBLICATIONS SUR:**www.cybermalveillance.gouv.fr