

Projet 1 - Un peu plus de sécurité, on n'en a jamais assez !

Que faire si votre ordinateur est infecté par un virus

1/ Exercice(s) pour vérifier la sécurité en fonction de l'appareil utilisé ???????
Comment faire ?

La façon la plus rapide, la plus simple et la plus sûre de détecter et de [supprimer des virus](#) ou autres malwares est d'utiliser un outil spécial tel qu'AVG Antivirus Gratuit. Vous pouvez aussi supprimer les [malwares et les applications malveillantes de votre smartphone](#) avec notre application mobile.

Comment installer un antivirus sur Windows



Quelque soit l'[antivirus que vous avez choisi](#), l'installation et la configuration sur un appareil Windows est assez similaire. Voici comment faire :

1. Créez un compte

Il n'est pas toujours nécessaire de créer tout de suite un compte, mais cela sera pratique sur le long terme. Avec certains éditeurs il n'est pas nécessaire de s'inscrire immédiatement, mais cela sera requis dans les 30 jours suivants l'achat. Créer un compte vous donnera un accès direct aux mises à jour, et à vous permettra de gérer vos licences et d'autres fonctionnalités, comme les fonctionnalités antiviol à distance pour votre appareil mobile, en un seul lieu.

3. Téléchargez l'antivirus

Cliquez pour télécharger l'antivirus. Il vous indiquera généralement l'espace requis, vous aurez donc peut-être besoin de supprimer des fichiers pour libérer de l'espace.

4. Autorisez les modifications

Il est également crucial de vérifier que vous disposez des privilèges administrateur, car vous devrez autoriser l'installation du logiciel. Cette étape nécessite que vous renseigniez votre mot de passe via un compte administrateur. Cela semble compliqué, mais il y a de fortes chances que vous soyez déjà l'administrateur et que Windows autorise simplement l'installation lorsque vous la lancerez. Essayez, tout simplement.

5. Suivez le processus d'installation décrit à l'écran

Le logiciel vous guidera ensuite à travers un court processus d'installation, qui implique généralement d'accepter les conditions générales d'utilisation et de définir où l'antivirus sera enregistré. L'installateur vous présentera ces étapes.

6. Redémarrez votre ordinateur

La version que vous avez téléchargée peut ne pas être la plus récente. Redémarrez simplement votre ordinateur, ce qui affichera toutes les mises à jour à installer. Une fois que c'est chose faite, effectuez une analyse complète de votre ordinateur – [voir nos conseils plus bas](#).

Comment installer un antivirus sur Mac



Du fait de la protection offerte aux utilisateurs de Mac par des éléments comme Gatekeeper, vous pourriez imaginer être protégé des virus, mais les Mac restent vulnérables aux chevaux de Troie, aux arnaques par hameçonnage et autres publiciels, comme Crossrider et des programmes embarqués, comme Mac Auto Fixer.

Mais si vous installez un programme antivirus pour Mac, nous supposons que vous êtes déjà au courant des menaces. Une fois que vous avez trouvé un antivirus ou une suite de sécurité compatible avec Mac ([consultez nos recommandations ici](#)), suivez les [mêmes étapes que pour un PC sous Windows](#).

Une fois l'installation terminée, lancez une analyse !

Une fois que vous avez installé votre logiciel antivirus, vous devrez **lancer une analyse pour chercher des menaces**. La plupart des suites de sécurité

proposent trois options d'analyse, manuelles ou automatiques, fournissant différents niveaux d'analyse :

1. Une analyse rapide

Les analyses rapides prennent généralement 10 à 20 minutes, car **elles n'examinent que les zones les plus susceptibles d'être infectées**. Cela permet au scanneur de contourner la majorité de votre réseau, ce qui réduit la vitesse, mais également la puissance de calcul, vous devrez donc arrêter d'utiliser votre ordinateur pendant son exécution. Souvent, cette option est suffisante pour mettre en lumière toutes les menaces.

2. Une analyse complète

Si votre analyse rapide n'a rien détecté, mais que vous pensez que votre ordinateur court toujours un risque, effectuez une analyse complète. Cette option **vérifie chaque recoin de votre système** pour vérifier qu'il ne comprend aucun virus et peut prendre plusieurs heures. Les menaces complexes, comme les logiciels espions peuvent ne pas être mises évidence par une analyse rapide et une analyse en profondeur pourra être nécessaire pour les détecter. Bien qu'une analyse complète soit l'option la plus lente, elle **garantira que votre disque est sain**.

3. Une analyse programmée

Les analyses programmées vérifient automatiquement vos fichiers à la recherche de virus à mesure que vous les utilisez, offrant une protection en temps réel à votre machine. **La majorité des produits antivirus proposent des analyses programmées par défaut**, mais il est possible de modifier la fréquence (quotidienne, hebdomadaire ou mensuelle) et l'heure dans les paramètres, si vous préférez qu'elles s'effectuent à des moments spécifiques, comme dans la nuit, lorsque vous n'utilisez pas votre appareil.

Protégez-vous contre la cybercriminalité

De nombreux antivirus pour [Windows](#) ou [Mac](#) sont faciles à utiliser, télécharger, et installer, il n'y a donc aucune raison de laisser votre ordinateur ou votre réseau

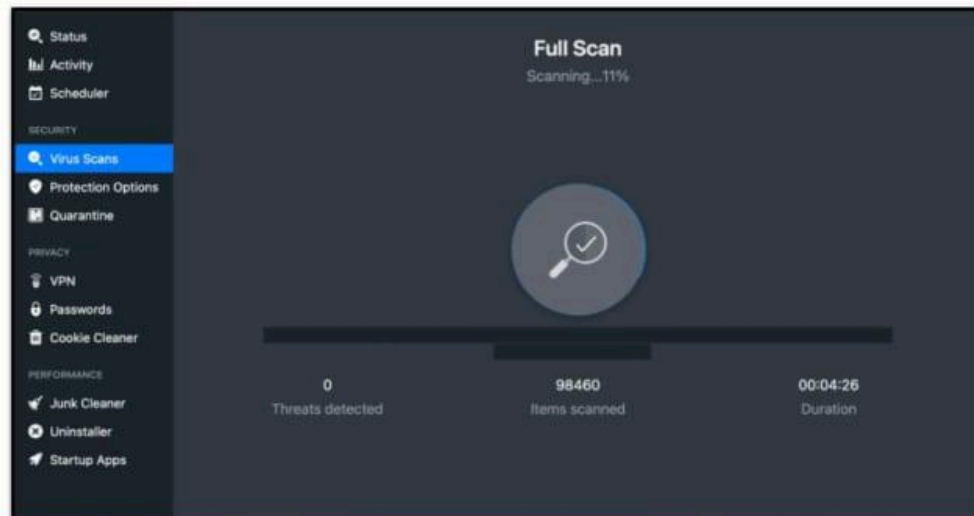
vulnérable. Vous recherchez toujours un bon antivirus à installer sur votre appareil ? [Découvrez quel est actuellement l'antivirus le mieux noté.](#)

2 / Exercice pour installer un antivirus + antimalware en fonction de l'appareil utilisé.

[Avira Prime](#) — Le meilleur pour les analyses rapides et les mises à jour automatiques de logiciels



L'offre *Prime* d'Avira combine un puissant scanner antivirus avec de nombreuses fonctionnalités utiles, dont un très bon outil de mise à jour des logiciels Windows. À l'instar de [Bitdefender](#), Avira utilise une technologie basée sur le cloud pour analyser vos appareils en ralentissant le moins possible votre système. Il a obtenu un taux de détection de 100 % face à des échantillons de logiciels malveillants anciens et récents. Le scanner d'Avira a également été le plus rapide lors de mes tests, terminant des analyses complètes en 20 minutes sur mon PC de jeu de 500 Go.



Le scanner d'Avira basé sur le cloud est très rapide

En plus de son scanner antivirus de pointe, Avira offre :

Un bouclier PUA. Vous protège contre les applications potentiellement indésirables (ou « potentially unwanted applications », PUA) pouvant être cachées dans des logiciels.

Un gestionnaire de pare-feu. Il optimise les paramètres du firewall selon le niveau de sécurité souhaité.

Une protection web. Vous protège contre toutes sortes de contenus malveillants et de sites de phishing.

Un VPN. Masque votre adresse IP derrière un serveur crypté pour plus de confidentialité en ligne.

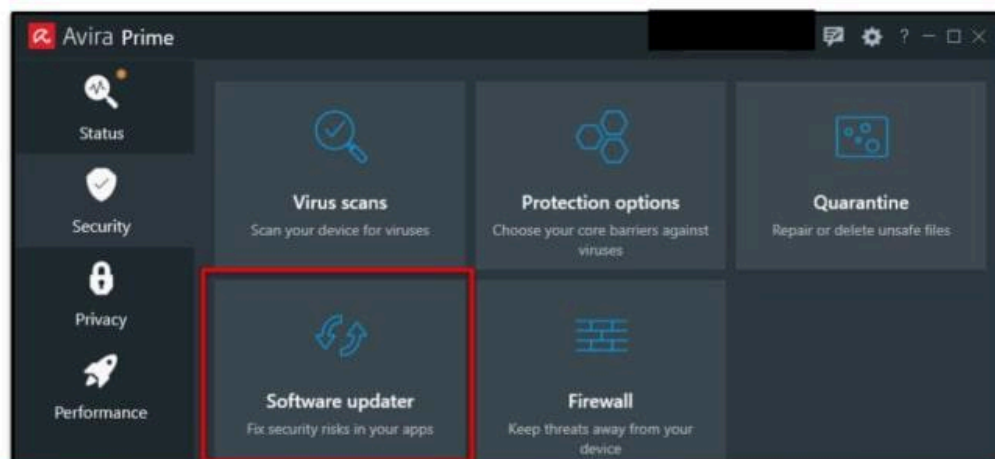
Un gestionnaire de mots de passe. Génère, stocke et remplit automatiquement vos identifiants pour plus de sécurité et de simplicité.

Un outil de mise à jour. Met automatiquement à jour de nombreux programmes populaires.

Des outils d'optimisation système avancés. Enregistre des données de performance complète, élimine les fichiers indésirables, améliore le délai de démarrage et optimise les performances de votre PC quand vous jouez.

J'aime beaucoup les fonctionnalités de réglage du système d'Avira, qui m'ont permis d'améliorer les performances sur l'un de mes anciens PC de test (qui

fonctionne toujours sous Windows 8). Le nettoyeur de fichiers inutiles a identifié plus de 1 Go de fichiers inutiles, et il a également signalé d'autres anciens fichiers que j'aurais pu vouloir conserver, en me laissant le choix de les supprimer ou non. J'apprécie vraiment cette approche, car elle permet de s'assurer que rien d'important n'est accidentellement supprimé de votre PC. Je suis également ravi que Software Updater détecte les programmes obsolètes et les mette automatiquement à jour.



Avira Software updater met automatiquement à jour les applications obsolètes susceptibles de présenter des vulnérabilités

Le gestionnaire de mots de passe d'Avira est l'une des applications les plus intuitives du marché, et la plupart de ses fonctionnalités sont disponibles gratuitement, notamment le stockage illimité de mots de passe, la synchronisation multi-appareils, l'enregistrement et le remplissage automatiques, et l'authentification à deux facteurs. Il s'agit sans aucun doute de l'un des meilleurs gestionnaires de mots de passe associé à un antivirus du marché.

Mon seul problème avec Avira est que son VPN n'est pas aussi rapide que celui de [Bitdefender](#), et qu'il ne fonctionne pas avec les sites de streaming les plus courants comme Netflix, Amazon Prime et Disney+. Cela dit, il dispose d'un kill switch pour les utilisateurs de Windows et prend en charge le torrenting, ce qui en fait un excellent choix dans la catégorie des VPN avec antivirus.

Avira ne propose pas non plus la surveillance du dark web ni de logiciel de contrôle parental, ce qui fait de [Norton](#) un meilleur choix si vous recherchez ces outils au sein de votre pack de sécurité Internet.

Avira propose plusieurs forfaits, mais mon préféré est Avira *Prime* (36,99 \$US / année), qui inclut le VPN Phantom d'Avira (avec des données de navigation illimitées) et protège jusqu'à 5 appareils Windows, macOS, Android ou iOS. Avira propose également [le meilleur antivirus gratuit du marché](#), mais il lui manque un grand nombre des fonctionnalités supplémentaires les plus importantes que l'on retrouve dans la version *Prime*. Toutes les formules payantes sont assorties d'une garantie de remboursement de 60 jours.

[Malwarebytes](#) – Idéal pour une protection basique en matière de cybersécurité



Malwarebytes est un antivirus simple qui affiche un bon taux de détection de malwares – lors de mes tests, l'antivirus à la demande de Malwarebytes a détecté environ 95 % des malwares testés, ce qui est correct sans être parfait comme dans le cas de [Norton](#) et de [Bitdefender](#). Cependant, sa protection en temps réel est plus impressionnante. Il a bloqué près de 99 % de ces mêmes fichiers – un score équivalent à certains des plus grands noms de l'industrie comme [TotalAV](#).

Malwarebytes dispose également d'une bonne extension de navigateur pour la sécurité web, Browser Guard, qui bloque les traqueurs, les publicités pop-up, les attaques et les sites de phishing. Elle s'est très bien comportée lors de mes tests, bloquant plus de 90 % des sites malveillants auxquels j'ai tenté d'accéder.

J'apprécie également le fait que vous puissiez facilement ajuster vos paramètres, par exemple si Malwarebytes bloque un site que vous savez sûr.



Cependant, j'ai été beaucoup moins impressionnée par le bloqueur de publicités de Malwarebytes. Ses performances sont médiocres par rapport à celui [d'Avira](#), car il laisse apparaître des publicités sur de nombreux sites que j'ai visités pendant mes tests.

Malwarebytes inclut un VPN, mais il n'est pas aussi riche en fonctionnalités que certains [VPN autonomes concurrents](#). Ce n'est pas non plus un excellent choix pour accéder à des sites de streaming populaires comme Netflix. Mais si tout ce que vous recherchez est un VPN facile à utiliser offrant des vitesses rapides, c'est un bon choix.

Malheureusement, Malwarebytes ne propose pas de fonctionnalités supplémentaires que l'on pourrait retrouver chez la plupart des autres antivirus haut de gamme, comme un pare-feu, un gestionnaire de mots de passe ou un outil de réglage du système. Cela dit, son design minimaliste et son manque de fonctionnalités supplémentaires peuvent séduire les utilisateurs à la recherche d'un programme antivirus simple.

Proposé à partir de 59,99 \$US / année, Malwarebytes est vendu au même prix que [Norton](#) et [Bitdefender](#), qui offrent tous deux des protections de cybersécurité bien plus complètes. Mais si vous êtes intéressé, Malwarebytes propose une garantie de remboursement sous 60 jours, il n'y a donc aucun risque à essayer.