

Avast! : réglez le logiciel

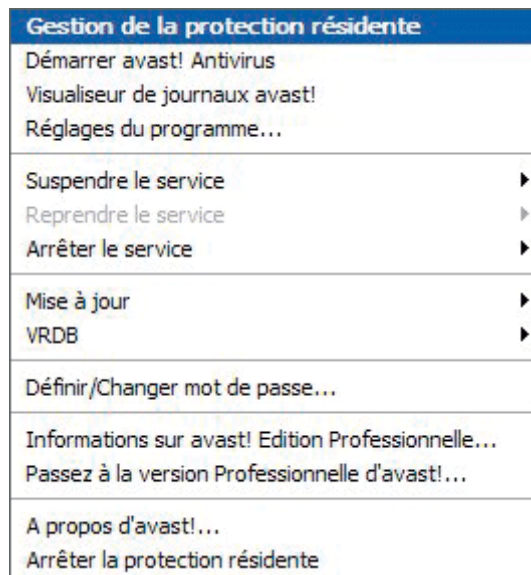
L'interface du programme peut dérouter car elle est découpée en plusieurs modules. Mais il n'y a rien de très compliqué malgré tout. Suivez le guide !

Roger Bouchez , Micro Hebdo (n° 492), le 28/09/2007 à 07h00

Réglez le module principal de façon optimale

De prime abord, Avast! peut dérouter à cause de son interface différente de celle des autres antivirus. En effet, il la « découpe » en plusieurs modules. Le plus important est le module de protection résidente (il assure la protection en temps réel du micro), qu'il faut régler avec attention.

Cliquez du bouton droit de la souris sur l'icône d'Avast! en bas à droite de l'écran, et sélectionnez **Gestion de la protection résidente :**



Une fenêtre nommée **Scanner résident** s'affiche. Cliquez sur le bouton **Détails** pour avoir accès à tous les réglages.

Nous allons détailler comment régler chacun des éléments (appelés boucliers). Une fois vos réglages effectués, cliquez sur **OK** pour fermer cette fenêtre.

Bouclier Peer2Peer

Cette protection n'est utile que si vous utilisez des programmes dits de *peer to peer*, comme BitTorrent ou TribalWeb.

Si ce n'est pas le cas, désactivez ce bouclier en cliquant sur le bouton **Terminer**, puis sur **Oui**. Pour réactiver un module désactivé, il suffit de cliquer sur le bouton **Démarrer**, situé sous le curseur du module, puis de confirmer par **Oui**.

Si vous utilisez ces logiciels pourvoyeurs de virus, réglez le curseur sur **Elevée**. Vous pouvez aussi cliquer sur **Personnaliser** afin d'adapter la surveillance aux seuls logiciels que vous utilisez.



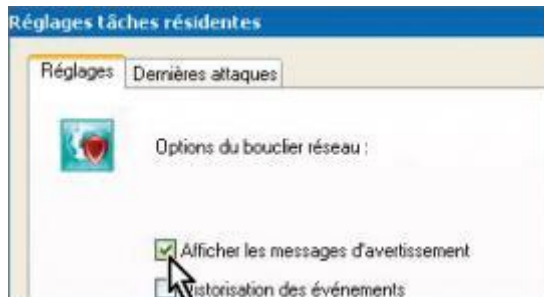
[Cliquez ici pour agrandir l'image](#)

Dans la fenêtre qui s'ouvre, cochez ou décochez les cases correspondantes et cliquez sur **OK**.

Bouclier réseau

Ce bouclier empêche la propagation des virus provenant d'Internet vers les différents micros de votre réseau.

Il est inutile de changer son niveau de protection, car les options **Normal** ou **Elevée** ne changent rien à son fonctionnement. En revanche, il est possible d'afficher ou non les alertes éventuelles en cliquant sur le bouton **Personnaliser**, puis en cochant ou décochant la case **Afficher les messages d'avertissement**.



[Cliquez ici pour agrandir l'image](#)

Bouclier Standard

Sa mission est d'analyser tous les logiciels ou fichiers qui sont lancés sur le PC.

S'il découvre un virus, il bloque son fonctionnement ou son ouverture. Choisissez l'option **Elevée** qui vérifie tous les fichiers alors que l'option **Normal** se contente des 57 formats les plus courants. Cela vous évite aussi de devoir vous perdre dans les nombreuses options de personnalisation. Enfin, il va de soi qu'il ne faut jamais désactiver ce bouclier... à moins d'avoir un bon motif pour le faire.



[Cliquez ici pour agrandir l'image](#)

Bouclier Web

Ce bouclier est l'un des plus importants d'Avast! car il est en première ligne dans la lutte antivirale alors que le bouclier Standard n'est en quelque sorte qu'un second rideau de défense.

Il permet, par exemple, d'intercepter les virus cachés dans des archives aux formats Zip ou Rar avant même qu'elles ne soient téléchargées sur votre micro (là où d'autres antivirus ne les analysent que lors de leur ouverture). Le niveau de sensibilité qui s'impose est bien évidemment **Elevée**.

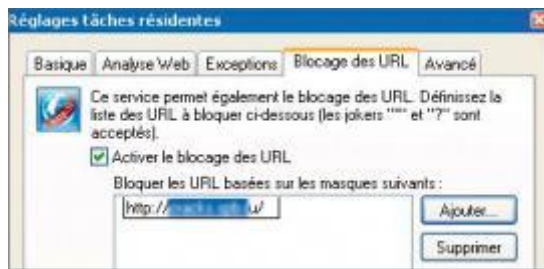


[Cliquez ici pour agrandir l'image](#)

Ce réglage a pour effet d'activer toutes les options de personnalisation du bouclier. Mais vous pouvez tout de même aller plus loin dans la protection en interdisant l'accès à certains sites que vous savez pourvoyeurs de virus. Cela élimine définitivement le risque de télécharger par mégarde un fichier infecté de ce site ou, pire encore, de télécharger un fichier qui serait infecté par un virus encore inconnu d'Avast!.

Avast! : réglez le logiciel

Pour mettre en place cette protection supplémentaire, cliquez sur le bouton **Personnaliser** puis sélectionnez l'onglet **Blocage URL**. Là, cochez la case **Activer le blocage des URL**, puis cliquez sur le bouton **Ajouter**. Tapez alors l'adresse du site en question et cliquez sur **OK**.



[Cliquez ici pour agrandir l'image](#)

Désormais, si par erreur vous allez sur ce site, un message d'erreur s'affichera :



[Cliquez ici pour agrandir l'image](#)

Courrier électronique

Ce module est destiné à vous protéger des risques liés à l'arrivée de virus via votre messagerie.

Ces infections sont parmi les plus fréquentes et les plus contagieuses, puisqu'elles peuvent se répandre via les carnets d'adresses. Il ne faut bien entendu jamais désactiver cette protection. Par défaut, elle est placée sur l'option **Normal**, ce qui est suffisant. Le placement du curseur sur **Elevée** aura pour seul effet d'augmenter à son niveau maximal la sensibilité **heuristique** de la détection, avec, comme gros inconvénient, un risque élevé de fausses alertes.

Parmi les autres réglages possibles, vous pouvez rassurer vos correspondants en faisant en sorte que les messages que vous leur envoyez affichent une information indiquant que le courriel a été vérifié par Avast! et qu'il est sain. Pour cela, cliquez sur le bouton **Personnaliser** puis, dans la fenêtre qui s'affiche, cochez la case **Insérer une note dans un message sain** :



[Cliquez ici pour agrandir l'image](#)

Répétez l'opération avec les autres onglets nommés **SMTP** et **IMAP**, puis cliquez sur **OK**.

Messagerie instantanée

Ce module n'a d'intérêt que si vous utilisez un logiciel de messagerie instantanée tel que Windows Live Messenger ou encore Yahoo! Messenger.

Réglez la protection sur **Elevée**, puis cliquez sur **Personnaliser**. Dans la fenêtre qui suit, ne gardez que les cases cochées des logiciels que vous utilisez.



[Cliquez ici pour agrandir l'image](#)

Si vous n'utilisez pas ce genre de logiciel, désactiver ce bouclier cliquant sur **Terminer**, puis sur **Oui**.

Outlook/Exchange

Ce bouclier n'est utile que si vous utilisez le logiciel de messagerie « professionnel » Outlook, livré avec la suite Office de Microsoft. Dans ce cas, réglez le curseur sur **Elevée**.

Si vous vous contentez de logiciels comme Outlook Express, Windows Mail, Windows Live Mail ou Thunderbird, vous pouvez désactiver ce module en cliquant sur le bouton **Terminer**, puis sur **Oui**.

Qu'est-ce que c'est ?

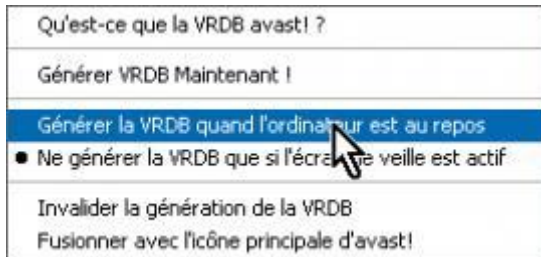
Heuristique

Méthode de détection des virus dont la signature n'est pas connue. L'analyse heuristique prend en compte le comportement des fichiers. Cette base d'analyse est sujette à plus d'erreurs que la méthode d'analyse sur base de données.

Réglez le fonctionnement de la VRDB

La VRDB, qu'est-ce que c'est ? Il s'agit d'une base de données, créée par Avast!, qui liste les fichiers présents sur le PC.

En cas d'infection sévère rendant un fichier inutilisable, son rôle est - comme son nom l'indique (VRDB signifiant *Virus Recovery Database*) -, de tenter de le remettre en l'état où il se trouvait avant l'infection. C'est pratique, mais gourmand en ressources. Le mieux est de cliquer du bouton droit de la souris sur l'icône de la VRDB (un petit **i** dans un rond bleu en bas et à droite de l'écran) pour sélectionner l'option **Générer la VRDB quand l'ordinateur est au repos**.



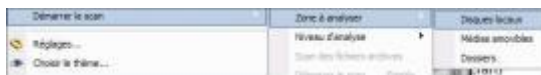
[Cliquez ici pour agrandir l'image](#)

Vous pouvez aussi arrêter cette fonction en cliquant, dans la même liste, sur **Invalidier la génération de la VRDB**. Enfin, profitez-en aussi pour faire disparaître l'icône de la VRDB en sélectionnant **Fusionner avec l'icône principale d'avast!**

Lancez une vérification manuelle

Quand vous souhaitez vérifier si un virus est présent sur un disque dur de votre ordinateur, cliquez avec le bouton de la souris sur l'icône d'Avast!, en bas à droite de l'écran, et sélectionnez **Démarrer avast! Antivirus**.

Dans la fenêtre principale du logiciel, cliquez n'importe où du bouton droit de la souris et sélectionnez **Démarrer le scan**, puis **Zone à Analyser** et enfin **Disques locaux**.



[Cliquez ici pour agrandir l'image](#)

Pour une analyse très poussée, cliquez sur l'icône en forme de disque dur en haut à droite puis, dans la petite fenêtre qui s'affiche en haut, faites glisser le curseur vers **Scan Minutieux** et cochez la case **Scan des archives**.

Cliquez n'importe où du bouton droit de la souris, et sélectionnez **Démarrer le scan** puis **Démarrer le scan**.



[Cliquez ici pour agrandir l'image](#)

Accédez aux options

Pour modifier certains réglages, il faut passer par la fenêtre des options. Elle est accessible en cliquant du bouton droit sur l'icône d'Avast!, en bas à droite de l'écran, et en sélectionnant **Réglages du programme**. Deux éléments principaux sont à régler.

Vérifiez la périodicité des mises à jour

Dans le menu de gauche, sélectionnez **Mise à jour (Général)** et vérifiez qu'à droite les éléments sélectionnés sont bien **Automatique** pour **Base de données virale** et **Demander lorsqu'une mise à jour est disponible** pour **Programme**. Le cas échéant, vous pouvez choisir une autre option dans celles indiquées. Cliquez sur **OK**.



[Cliquez ici pour agrandir l'image](#)

Avast! met à jour sa base de données de virus toutes les quatre heures.

Désactivez les alertes sonores

L'un des défauts d'Avast! est le dérangement régulièrement provoqué par les annonces de mise à jour de la base de virus ou du programme en lui-même. Pour supprimer ces alertes vocales pas très agréables, sélectionnez la ligne **Sons** dans le menu de gauche, puis cochez la case **Désactiver les sons d'avast!**.

Cliquez enfin sur **OK** pour valider.