Malwarebytes : Le guide essentiel pour protÃ©ger efficacement votre ordinateur

CatÃ©gorie : SÃ©curitÃ©
PubliÃ© par Nendo le 06/06/2026

Les menaces informatiques Ã©voluent constamment et peuvent compromettre la sÃ©curitÃ© de vos donnÃ©es personnelles en quelques instants. Pour renforcer la protection de votre ordinateur sous Windows, Malwarebytes figure parmi les solutions les plus apprÃ©ciÃ©es par les utilisateurs. Ce logiciel est conÃ§u pour dÃ©tecter et supprimer les logiciels malveillants, les programmes indÃ©sirables et diverses menaces pouvant Ã©chapper Ã un antivirus traditionnel. GrÃ¢ce Ã une interface claire et Ã des outils performants, il convient aussi bien aux dÃ©butants qu'aux utilisateurs expÃ©rimentÃ©s. DÃ©couvrez dans ce guide les Ã©tapes indispensables pour prendre en main Malwarebytes et sÃ©curiser votre systÃ¨me dÃ¨s les premiers jours d'utilisation.

1) TÃ©lÃ©charger et installer Malwarebytes

Rendez-vous sur la fiche du logiciel depuis le site NetFox2 pour **tÃ©lÃ©charger le logiciel Malwarebytes pour Windows**. Une fois le fichier obtenu, lancez l'installation et suivez les instructions affichÃ©es Ã l'Ã©cran. L'assistant d'installation configure automatiquement les paramÃ¨tres de base afin de permettre une utilisation rapide du logiciel.

2) Effectuer la configuration initiale

Au premier dÃ©marrage, Malwarebytes propose plusieurs options de protection. Prenez le temps de vÃ©rifier les rÃ©glages disponibles, notamment ceux liÃ©s Ã la dÃ©tection en temps rÃ©el, aux analyses programmÃ©es et aux notifications. Cette Ã©tape permet d'adapter le logiciel Ã vos besoins et Ã votre usage quotidien.

2.1 - **VÃ©rifier l'Ã©tat de la protection** : Depuis le tableau de bord principal, assurez-vous que les modules de protection disponibles sont activÃ©s. Les utilisateurs de la version Premium bÃ©nÃ©ficient notamment de la protection en temps rÃ©el contre les logiciels malveillants, les ransomwares et les sites web malveillants.
2.2 - **Configurer les mises Ã jour automatiques** : AccÃ©dez aux paramÃ¨tres du logiciel et vÃ©rifiez que les mises Ã jour automatiques sont activÃ©es. Malwarebytes pourra ainsi tÃ©lÃ©charger les derniÃ¨res dÃ©finitions de menaces sans intervention manuelle, garantissant une meilleure efficacitÃ© des analyses.
2.3 - **Personnaliser les analyses programmÃ©es** : Dans la section dÃ©diÃ©e Ã la planification, choisissez la frÃ©quence des analyses automatiques. Une analyse rapide quotidienne ou une analyse complÃ¨te hebdomadaire constitue gÃ©nÃ©ralement un bon compromis entre sÃ©curitÃ© et performances.
2.4 - **DÃ©finir les options de dÃ©tection** : Les paramÃ¨tres permettent d'ajuster le niveau de dÃ©tection des programmes potentiellement indÃ©sirables (PUP) et des modifications potentiellement indÃ©sirables (PUM). Pour une protection renforcÃ©e, il est conseillÃ© de sÃ©lectionner l'option qui demande une action ou met automatiquement ces Ã©lÃ©ments en quarantaine.
2.5 - **VÃ©rifier les exclusions si nÃ©cessaire** : Dans certains cas, des programmes lÃ©gitimes

peuvent Ãªtre signalÃ©s Ã tort. La section Â« Exclusions Â» permet d'ajouter des fichiers, dossiers ou applications de confiance afin qu'ils ne soient pas analysÃ©s ou bloquÃ©s par erreur.
2.6 - **Effectuer une premiÃ¨re analyse de contrÃ´le** : Une fois les rÃ©glages terminÃ©s, lancez une analyse de votre systÃ¨me. Cette vÃ©rification initiale permet de s'assurer qu'aucune menace n'est dÃ©jÃ prÃ©sente sur l'ordinateur et confirme que Malwarebytes fonctionne correctement.

3) Mettre Ã jour la base de donnÃ©es

Avant d'effectuer une analyse, assurez-vous que la base de signatures est Ã jour. Les mises Ã jour rÃ©guliÃ¨res permettent au logiciel de reconnaÃ®tre les menaces les plus rÃ©centes et d'amÃ©liorer son efficacitÃ© lors des analyses.

3.1 - **Ouvrez Malwarebytes** : depuis le menu DÃ©marrer ou l'icÃ´ne prÃ©sente sur le Bureau.
3.2 - **AccÃ©dez au tableau de bord principal** : La date de la derniÃ¨re mise Ã jour est gÃ©nÃ©ralement affichÃ©e dans la fenÃªtre d'accueil.
3.3 - **Recherchez les mises Ã jour disponibles** : en cliquant sur le bouton Â« **Rechercher les mises Ã jour** Â» ou Â« **VÃ©rifier les mises Ã jour** Â», selon la version du logiciel installÃ©e.
3.4 - **Patientez pendant le tÃ©lÃ©chargement** : Malwarebytes se connecte aux serveurs de l'Ã©diteur pour rÃ©cupÃ©rer les derniÃ¨res dÃ©finitions de menaces et les Ã©ventuelles amÃ©liorations du programme.
3.5 - **VÃ©rifiez le rÃ©sultat de l'opÃ©ration** : Une fois le processus terminÃ©, un message confirme que la base de donnÃ©es est Ã jour et affiche la date de la derniÃ¨re mise Ã jour.
3.6 - **Activez les mises Ã jour automatiques** : si cette option est disponible dans votre version. Pour cela, ouvrez les paramÃ¨tres du logiciel puis assurez-vous que les mises Ã jour automatiques sont activÃ©es afin que Malwarebytes tÃ©lÃ©charge les nouvelles dÃ©finitions sans intervention de votre part.

4) Lancer une analyse complÃ¨te du systÃ¨me

Une fois les mises Ã jour terminÃ©es, dÃ©marrez une analyse approfondie de l'ordinateur. Malwarebytes examine les fichiers, les applications et les zones sensibles de Windows afin d'identifier d'Ã©ventuels programmes malveillants. Selon la capacitÃ© de votre machine et la quantitÃ© de donnÃ©es stockÃ©es, cette opÃ©ration peut prendre un certain temps.

4.1 - **Ouvrez Malwarebytes** depuis le menu DÃ©marrer ou en cliquant sur son icÃ´ne dans la barre des tÃ¢ches.
4.2 - **AccÃ©dez Ã la section "Analyseur" ou "Scanner"** depuis le tableau de bord principal.
4.3 - **SÃ©lectionnez le type d'analyse** : Selon la version du logiciel, plusieurs options peuvent Ãªtre proposÃ©es. Choisissez l'analyse la plus approfondie disponible pour examiner l'ensemble du systÃ¨me.
4.4 - **VÃ©rifiez les Ã©lÃ©ments Ã analyser** : Si Malwarebytes vous permet de personnaliser l'analyse, assurez-vous que les disques locaux, la mÃ©moire systÃ¨me, les programmes de dÃ©marrage et les emplacements sensibles sont inclus.
4.5 - **Cliquez sur "Lancer l'analyse"** pour dÃ©marrer l'examen du systÃ¨me. Le logiciel commence alors Ã inspecter les fichiers et les processus en cours d'exÃ©cution.
4.6 - **Patientez jusqu'Ã la fin de l'analyse** : La durÃ©e dÃ©pend du volume de donnÃ©es stockÃ©es sur votre ordinateur, des performances de votre matÃ©riel et du nombre de fichiers Ã examiner.
4.7 - **Consultez les rÃ©sultats affichÃ©s une fois l'analyse terminÃ©e** : Malwarebytes prÃ©sente un rapport dÃ©taillant les menaces dÃ©tectÃ©es, les fichiers suspects et les

Ã©ventuelles actions recommandÃ©es.
4.8 - **Placez les Ã©lÃ©ments dÃ©tectÃ©s en quarantaine** ou supprimez-les selon les recommandations du logiciel. Cette Ã©tape permet d'empÃªcher les fichiers malveillants de nuire au systÃ¨me.
4.9 - **RedÃ©marrez l'ordinateur si nÃ©cessaire** : Certaines menaces ne peuvent Ãªtre supprimÃ©es complÃ¨tement qu'aprÃ¨s un redÃ©marrage de Windows.

5) Traiter les Ã©lÃ©ments dÃ©tectÃ©s

Ã€ l'issue de l'analyse, le logiciel affiche un rapport dÃ©taillÃ© des menaces identifiÃ©es. VÃ©rifiez les rÃ©sultats puis placez les Ã©lÃ©ments suspects en quarantaine ou supprimez-les selon les recommandations fournies. Cette action contribue Ã Ã©liminer les risques potentiels pour votre systÃ¨me.

5.1 - **Ouvrez le rapport d'analyse** : Ã€ la fin du scan, cliquez sur le bouton permettant d'afficher les rÃ©sultats. Vous y trouverez la liste complÃ¨te des Ã©lÃ©ments dÃ©tectÃ©s ainsi que leur niveau de risque.
5.2 - **Examinez les menaces identifiÃ©es** : Prenez connaissance des informations fournies pour chaque dÃ©tection. Malwarebytes indique gÃ©nÃ©ralement le type de menace concernÃ©e, son emplacement et l'action recommandÃ©e.
5.3 - **Laissez les Ã©lÃ©ments suspects sÃ©lectionnÃ©s** : Par dÃ©faut, les objets dÃ©tectÃ©s sont souvent cochÃ©s automatiquement. Cette sÃ©lection permet de traiter rapidement les menaces les plus courantes.
5.4 - **Placez les fichiers en quarantaine** : Cliquez sur l'option de mise en quarantaine pour isoler les Ã©lÃ©ments dÃ©tectÃ©s. Cette mÃ©thode est recommandÃ©e, car elle empÃªche l'exÃ©cution des fichiers suspects tout en conservant la possibilitÃ© de les restaurer en cas d'erreur.
5.5 - **Supprimez les menaces confirmÃ©es** : Si vous Ãªtes certain qu'un Ã©lÃ©ment est malveillant ou inutile, vous pouvez choisir de le supprimer dÃ©finitivement. Cette action libÃ¨re Ã©galement l'espace occupÃ© par les fichiers concernÃ©s.
5.6 - **RedÃ©marrez l'ordinateur si demandÃ©** : Certaines menaces Ã©tant actives pendant l'utilisation de Windows, Malwarebytes peut demander un redÃ©marrage afin de finaliser leur suppression.
5.7 - **Consultez la quarantaine rÃ©guliÃ¨rement** : La section Quarantaine permet de visualiser les Ã©lÃ©ments isolÃ©s. AprÃ¨s quelques jours sans problÃ¨me de fonctionnement, vous pouvez supprimer dÃ©finitivement les fichiers mis en quarantaine.
5.8 - **VÃ©rifiez l'Ã©tat du systÃ¨me** : Une fois les actions terminÃ©es, effectuez une nouvelle analyse pour confirmer que toutes les menaces ont Ã©tÃ© Ã©liminÃ©es et que le systÃ¨me est dÃ©sormais sain.

6) Planifier des analyses automatiques

Pour maintenir un niveau de sÃ©curitÃ© constant, programmez des analyses rÃ©guliÃ¨res. Une vÃ©rification automatique hebdomadaire ou quotidienne permet de dÃ©tecter rapidement les nouvelles menaces sans intervention manuelle.

6.1 - **Ouvrez Malwarebytes** : Lancez le logiciel depuis le menu DÃ©marrer ou l'icÃ´ne prÃ©sente sur votre Bureau.
6.2 - **AccÃ©dez aux paramÃ¨tres d'analyse** : Depuis l'interface principale, ouvrez la section dÃ©diÃ©e aux analyses ou Ã la planification des tÃ¢ches. L'emplacement exact peut varier selon la version installÃ©e.

6.3 - **CrÃ©er une nouvelle planification** : Cliquez sur l'option permettant d'ajouter ou de programmer une analyse automatique. Une fenÃªtre de configuration s'affiche alors.
6.4 - **Choisissez le type d'analyse** : SÃ©lectionnez l'analyse qui correspond le mieux Ã vos besoins :
- Analyse rapide pour un contrÃ´le frÃ©quent des zones les plus sensibles.
- Analyse complÃ¨te pour une vÃ©rification approfondie de l'ensemble du systÃ¨me.
6.5 - **DÃ©finissez la frÃ©quence d'exÃ©cution** : Malwarebytes permet gÃ©nÃ©ralement de programmer des analyses :
- **Quotidiennes** ;
- **Hebdomadaires** ;
- **Mensuelles**.
6.6 - **SÃ©lectionnez l'heure de lancement** : Programmez les analyses Ã un moment oÃ¹ l'ordinateur est habituellement allumÃ© mais peu sollicitÃ©, par exemple en dehors des heures de travail.
6.7 - **Enregistrez la tÃ¢che planifiÃ©e** : VÃ©rifiez les paramÃ¨tres choisis puis validez la configuration. L'analyse sera exÃ©cutÃ©e automatiquement selon le calendrier dÃ©fini.
6.8 - **ContrÃ´lez les rÃ©sultats rÃ©guliÃ¨rement** : Consultez les rapports gÃ©nÃ©rÃ©s aprÃ¨s chaque analyse afin de vÃ©rifier que les contrÃ´les se dÃ©roulent correctement et qu'aucune menace n'a Ã©tÃ© dÃ©tectÃ©e.

7) Surveiller la protection en temps rÃ©el

Si votre version de Malwarebytes inclut la protection en temps rÃ©el, assurez-vous qu'elle reste activÃ©e. Cette fonctionnalitÃ© surveille en permanence les activitÃ©s du systÃ¨me et bloque automatiquement les comportements suspects avant qu'ils ne causent des dommages.

7.1 - **Ouvrez Malwarebytes** : Lancez le logiciel depuis le menu DÃ©marrer ou Ã partir de l'icÃ´ne prÃ©sente dans la zone de notification de Windows.
7.2 - **Consultez le tableau de bord principal** : DÃ¨s l'ouverture du programme, l'Ã©cran d'accueil affiche l'Ã©tat des diffÃ©rents modules de protection. VÃ©rifiez que chaque protection disponible est indiquÃ©e comme active.
7.3 - **ContrÃ´lez les modules de sÃ©curitÃ©** : Selon votre version de Malwarebytes, plusieurs protections peuvent Ãªtre proposÃ©es (Chaque module doit Ãªtre activÃ© pour garantir une couverture optimale.) :
- **Protection contre les logiciels malveillants** ;
- **Protection contre les ransomwares** ;
- **Protection web contre les sites dangereux** ;
- **Protection contre les exploits**.
7.4 - **VÃ©rifiez les notifications de sÃ©curitÃ©** : Malwarebytes affiche gÃ©nÃ©ralement des alertes lorsqu'une menace est bloquÃ©e ou lorsqu'une intervention est nÃ©cessaire. Prenez l'habitude de consulter ces notifications afin de rester informÃ© des Ã©vÃ©nements importants.
7.5 - **Consultez les journaux d'activitÃ©** : La section dÃ©diÃ©e aux rapports ou Ã l'historique permet de visualiser les menaces dÃ©tectÃ©es, les sites bloquÃ©s et les actions rÃ©alisÃ©es automatiquement.
7.6 - **Surveillez l'icÃ´ne dans la barre des tÃ¢ches** : Lorsque la protection en temps rÃ©el est active, l'icÃ´ne Malwarebytes apparaÃ®t gÃ©nÃ©ralement dans la zone de notification de Windows. Une modification de son apparence ou l'affichage d'un avertissement peut signaler un problÃ¨me nÃ©cessitant votre attention.
7.7 - **VÃ©rifiez rÃ©guliÃ¨rement les mises Ã jour** : Une protection en temps rÃ©el n'est

pleinement efficace que si les bases de donnÃ©es et les composants du logiciel sont Ã jour. Assurez-vous que les mises Ã jour automatiques sont activÃ©es.
7.8 - **Tester le bon fonctionnement du logiciel** : Sans manipuler de fichiers dangereux, vous pouvez vÃ©rifier que Malwarebytes dÃ©tecte correctement les comportements suspects en consultant les alertes et les Ã©vÃ©nements enregistrÃ©s dans les journaux de sÃ©curitÃ©.

8) Consulter les rapports de sÃ©curitÃ©
Les journaux et rapports gÃ©nÃ©rÃ©s par Malwarebytes offrent une vue dÃ©taillÃ©e des analyses effectuÃ©es et des menaces neutralisÃ©es. Les consulter rÃ©guliÃ¨rement permet de mieux comprendre l'Ã©tat de sÃ©curitÃ© de votre ordinateur et d'identifier d'Ã©ventuels problÃ¨mes rÃ©currents.

En conclusion, Malwarebytes constitue un excellent complÃ©ment de sÃ©curitÃ© pour les utilisateurs de Windows souhaitant renforcer la protection de leur ordinateur. En suivant les Ã©tapes prÃ©sentÃ©es dans ce guide, vous pourrez installer le logiciel correctement, optimiser ses paramÃ¨tres et bÃ©nÃ©ficier d'une surveillance efficace contre les menaces numÃ©riques. Une utilisation rÃ©guliÃ¨re et des mises Ã jour frÃ©quentes contribueront Ã prÃ©server durablement la sÃ©curitÃ© de votre systÃ¨me et de vos donnÃ©es.