SÉCURITÉ & CONFIDENTIALITÉ

1

Sécurité avant tout ! Dans ce chapitre, nous verrons comment se protéger de manière efficace contre les virus et autres menaces numériques. Nous aborderons également la protection de votre vie privée et la réalisation d'un back-up en cas d'imprévu.

Avant d'aborder Windows, il est essentiel de sécuriser votre système. Les menaces sont nombreuses, surtout lorsque vous surfez sur internet. Il ne s'agit pas uniquement de virus qui rendent votre ordinateur inutilisable. Il existe d'autres menaces numériques. Cette liste détaille les risques les plus courants :

• **Phishing (hameçonnage)**

Les criminels tentent d'obtenir des données bancaires et confidentielles à l'aide de faux e-mails, SMS ou messages instantanés. Ils utilisent ensuite ces données pour des activités illicites, comme par exemple vider votre compte bancaire.

• **Malware (logiciel malveillant)**

Les criminels subtilisent votre numéro de carte de crédit ou d'autres données confidentielles en installant un logiciel malveillant sur votre ordinateur. Ils les utilisent ensuite pour vous dérober de l'argent. Le terme "malware" regroupe les infections informatiques comme les virus et les chevaux de Troie.

• **Ransomware (rançongiciel)**

Aussi appelé logiciel de rançonnage. Avec ce type de malware, les criminels dérobent des fichiers qui se trouvent sur votre disque dur et ne vous les rendent qu'après le paiement d'une rançon (voir encadré "Ne payez pas de rançon !").

• **Rootkit**

Ce malware se niche au plus profond du système d'exploitation, ce qui rend sa détection et sa suppression difficiles. Un rootkit peut être responsable de l'instabilité du système.

• **Adware (publiciel)**

Moins dangereux, mais tout aussi gênant, ce type de logiciel affiche des publicités supplémentaires lorsque vous êtes sur des sites web, par exemple sous la forme de pop-ups indésirables. Les concepteurs de l'adware espèrent ainsi bénéficier de revenus supplémentaires.

• **Spyware (logiciel espion)**

Programme qui collecte des informations sur l'utilisateur de l'ordinateur. Il peut s'agir d'un enregistreur de frappe destiné à subtiliser les données d'une carte de crédit, mais l'espion numérique peut également être en quête d'informations pour afficher des publicités ciblées.

• **Sites web à risque**

Les sites web de moindre ampleur sont tout particulièrement la cible de pirates et peuvent – souvent à leur insu – répandre des logiciels malveillants. Ils peuvent également diffuser des publicités contenant du code dangereux.

• **Programmes indésirables**

Lors de l'installation d'un logiciel, il arrive souvent qu'un programme non désiré soit installé en plus sur votre ordinateur. Certains logiciels installent aussi une barre d'outils (barre de boutons) non désirée pour le navigateur.

• **Les annonceurs indiscrets**

Pour que les publicités correspondent aux intérêts des personnes qui visitent les sites web, certains annonceurs établissent le profil des utilisateurs. Il s'agit d'une atteinte à la vie privée, puisque ces derniers ne sont pas mis au courant.

Ne payez pas de rançon !

Vous êtes victime d'un ransomware ? Ne payez pas de rançon. Il se pourrait que vous ne receviez aucune clé de la part des cybercriminels pour déverrouiller votre ordinateur. De plus, en payant, vous encouragez ces pratiques criminelles. Rendez-vous sur **www.nomoreransom.org** pour voir quelles sont vos options. Il s'agit d'un site de la police, d'Europol, de Kaspersky et d'Intel. Cependant, contre le ransomware, rien ne vaut un bon back-up.

Windows vous propose heureusement des solutions pour lutter contre ce type de menace numérique. Un antivirus (chp. 1.1 et 1.2) peut par exemple protéger votre ordinateur des malwares et un back-up (chp. 1.4) vous permettra de restaurer votre système en cas de pépin. Vous pouvez également protéger vos données confidentielles à l'aide d'une série de mesures. Il est par exemple possible de modifier les paramètres de Windows de façon à ce que moins d'informations personnelles soient envoyées à Microsoft (chp. 1.3).

Surfez en toute sécurité

Vous trouverez d'autres conseils pour surfer en toute sécurité dans notre guide **Sécurité en ligne – 80 astuces pour se protéger (réf. 149).** En tant qu'abonné à Test Achats, vous ne payez que 1,95 € de frais administratifs. Passez commande au 02 290 34 85 ou sur **testachats.be/guidespratiques**.

1.1 WINDOWS DEFENDER

Afin d'utiliser Windows 10 en toute sécurité, il est essentiel de se protéger contre les logiciels malveillants. Le système dispose d'un antivirus intégré, Windows Defender, qui constitue le strict minimum en matière de protection contre les malwares. Nos tests montrent que des antivirus produits par d'autres développeurs sont plus performants (consultez les résultats sur **www.testachats.be/comparerantivirus**). Si vous ne voulez pas d'un autre antivirus, vous devriez au minimum utiliser Windows Defender.

1.1a Activer Windows Defender

Windows Defender est automatiquement activé si aucun autre antivirus n'est installé. Une vérification s'impose néanmoins pour plus de sécurité.

Windows Defender

1 Cliquez sur Rechercher (voir encadré "Lancer un programme via Rechercher") et tapez "Sécurité Windows".
2 Cliquez sur le premier résultat pour ouvrir le centre de sécurité de Windows Defender.
3 Passons en revue plusieurs fonctions intéressantes :
• **Protection contre les virus et les menaces** : l'antivirus intégré est automatiquement activé lorsque vous n'installez pas votre propre antivirus ou lorsqu'il a expiré.
• **Pare-feu et sécurité réseau** : le pare-feu intégré est automatiquement activé si aucun pare-feu n'est installé
• **Gestion des applications et des navigateurs** : gère les paramètres de Windows Defender Smartscreen, la protection intégrée à Windows et Edge contre les programmes et sites web malveillants. Choisissez l'option "Avertir" pour chaque élément. Vous serez averti lorsque vous risquez d'ouvrir un programme ou un site web nuisible.
• **Performances et état de l'appareil** : vous trouverez ici des informations sur l'état de votre PC (si votre système est à jour, s'il y a des problèmes avec la batterie, etc.). En cas de souci, les actions à prendre sont détaillées.

Lancer un programme via "Rechercher"

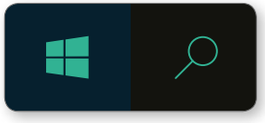
Dans ce guide, nous utilisons la fonction "Rechercher" pour lancer des programmes ou trouver certains paramètres. Pour ce faire, cliquez sur l'icône de recherche (la loupe située à côté du logo de Windows), située en bas à gauche de votre écran, dans la barre des tâches. Tapez ensuite le nom du programme ou du paramètre désiré. La fonction "Rechercher" de Windows se charge alors de trouver le programme en question. Il est aussi possible de trouver des programmes ou des paramètres via la liste des programmes dans le menu Démarrer. Les paramètres sont également accessibles via les menus "Paramètres" et "Panneau de configuration". Si vous utilisez régulièrement certains programmes ou paramètres, vous pouvez les épingler au menu Démarrer (voir chp. 5.1a) ou à la barre des tâches (voir chp. 5.3).

1.1b Moins de notifications

Les notifications de Windows Defender apparaissent dans le Centre de notifications. C'est là où aboutissent tous les messages dans Windows. Nous aborderons cet élément en profondeur plus loin dans cet ouvrage (voir chp. 5.10). Si vous estimez voir apparaître trop de notifications de Windows Defender, vous pouvez facilement les désactiver.

1.1c Analyse complète

Windows Defender dispose de toutes sortes d'analyses. Si vous désirez effectuer un simple contrôle des infections, optez pour l'analyse rapide. Le logiciel contrôlera alors les emplacements et fichiers les plus exposés. Dans la section "Protection contre les virus et les menaces", cliquez sur "Analyse rapide".



Windows Defender

1 Lancez Windows Defender et cliquez en bas à gauche sur "Paramètres".
2 Dans Gérer les notifications, sélectionnez les notifications que vous voulez recevoir (si vous le souhaitez, réglez le curseur sur "Désactivé" en le déplaçant vers la gauche).

Pour contrôler votre ordinateur de fond en comble, sélectionnez l'analyse complète (cliquez sur "Options d'analyse", sélectionnez "Analyse complète" puis choisissez "Analyser maintenant"). A la première utilisation du logiciel, il est conseillé de procéder à cette analyse complète. Par après, vous pourrez généralement vous contenter de l'analyse rapide, bien qu'il soit recommandé d'en effectuer une complète de temps à autre.

1.1d Optez pour l'analyse hors ligne en cas de malware persistant

L'analyse complète ne constitue pas l'option la plus radicale. Windows Defender vous propose également une analyse hors ligne. Celle-ci se révèle utile si votre ordinateur est infecté par un malware ou un rootkit difficile à supprimer. Vous aurez plus de chances de l'éliminer si l'ordinateur est démarré dans un mode spécial via l'analyse hors ligne. Sélectionnez "Analyse Windows Defender hors ligne" et cliquez sur "Analyser maintenant".

1.1e Afficher les virus détectés

Après avoir effectué l'analyse, vous désirerez certainement en connaître les résultats. Vous les trouverez dans Windows Defender sous "Protection contre les virus et menaces". Cliquez sur "Historique de protection" pour obtenir un aperçu des menaces trouvées.

1.1f Notifications concernant un malware

Si un virus est repéré, une notification sera envoyée au "Centre de notifications".

1.2 CHOISIR UN MEILLEUR ANTIVIRUS

Windows Defender n'est certainement pas l'antivirus le plus performant. De nombreuses personnes l'utilisent parce qu'il est livré gratuitement avec Windows, mais nos tests ont montré que sa protection contre les malwares reçoit tout juste un "bon" score. D'autres antivirus gratuits lui sont parfois supérieurs, mais ils n'atteignent pas le niveau de leurs homologues payants. En outre, les antivirus gratuits vous bombardent souvent de publicités intempestives pour leur version payante et vous devez parfois vous contenter d'un logiciel en anglais (par exemple Bitdefender Free).
Pour votre confort, il est donc conseillé d'opter pour un package payant. Pour découvrir celui qui vous convient le mieux, vous avez la possibilité d'utiliser la plupart des antivirus gratuitement pendant une période d'essai. Il est toutefois déconseillé d'installer plusieurs versions d'essai d'affilée. En effet : lors de sa désinstallation, un antivirus laisse derrière lui des éléments qui, à terme, risquent de ralentir votre ordinateur.

1.2a Bitdefender (payant) et Eset

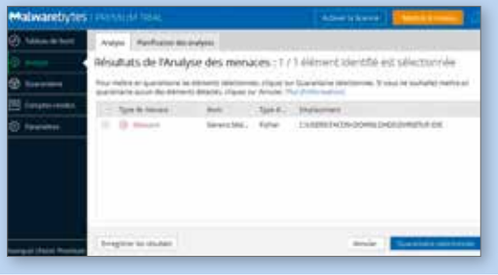
D'après notre dernier test, les antivirus gratuits de Bitdefender (Maître-Achat) et Avast présentent une protection supérieure, mais ce sont Eset et la version payante de Bitdefender (Meilleur du Test) qui proposent le moins de risques d'infection par des malwares et d'autres menaces.

Si vous désirez mettre à niveau vers Windows 10 un ancien ordinateur avec peu de mémoire, vous pouvez opter pour Eset Internet Security. Cet antivirus utilise peu de mémoire et vous permettra de bénéficier d'une protection avancée.

Les deux antivirus sont également une bonne option si vous souhaitez mettre à niveau vers Windows 10 un PC plus ancien avec peu de mémoire. Ils combinent une excellente protection avec une faible charge (utilisation de mémoire) sur votre ordinateur.

Deuxième avis

D'autres programmes peuvent faire office de deuxième ligne de défense en plus de votre antivirus principal. De nombreux utilisateurs installent Malwarebytes Anti-Malware (fr.malwarebytes.com) ou HitmanPro (www.hitmanpro.com) pour bénéficier d'une protection supplémentaire contre les malwares. Ces programmes sont également capables d'éliminer les menaces. Si vous optez pour Malwarebytes Anti-Malware, assurez-vous d'installer la version gratuite.



1.2b Les comptes d'utilisateurs

Avant de pouvoir utiliser Windows 10, il vous faudra créer un compte. Microsoft vous encourage à créer un compte Microsoft, par exemple une adresse e-mail qui termine par "hotmail.com". Cela présente certains avantages. Vous pourrez utiliser les applications Courrier, Calendrier et OneDrive directement, sans

Ça vaut la peine de comparer

Lors de l'achat d'un antivirus, il est utile de comparer les prix de différentes boutiques (en ligne). Bizarrement, un antivirus en boîte vendu en magasin est parfois moins cher que sa version téléchargeable, même s'il ne contient qu'un code qui vous fait accéder à... la version téléchargeable !

Ces antivirus sont parfois présentés avec une réduction considérable, surtout lorsque leur licence arrive à terme. Pour éviter de se faire avoir, il est important d'acheter chez un fournisseur fiable.

configuration supplémentaire. Vous pourrez également télécharger des applis via le Windows Store.

Si vous n'avez pas besoin d'un compte Microsoft, vous pouvez également opter pour un compte local. Pour utiliser par la suite un service Microsoft comme OneDrive ou Skype, il faudra vous y connecter séparément.

Administrateur

Le premier compte dispose toujours des droits d'administrateur, qui vous garantissent tous les droits de gestion, comme l'installation d'un logiciel, la modification des paramètres du système ainsi que d'autres réglages importants.

Il est déconseillé d'octroyer les droits d'administrateur aux autres comptes. Optez plutôt pour des comptes standard.

Utilisateurs multiples

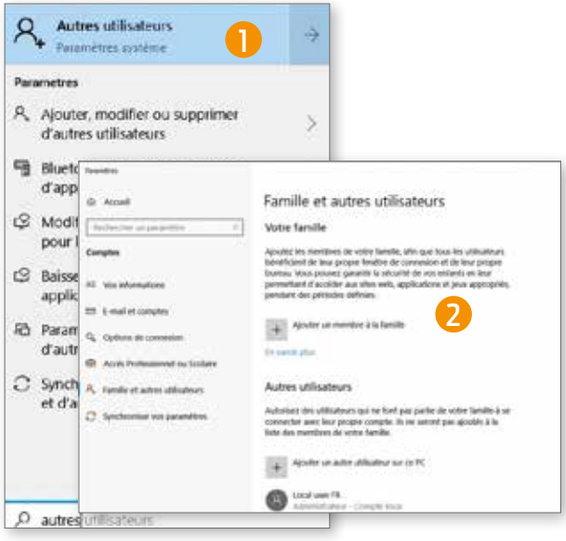
La création de comptes d'utilisateurs supplémentaires s'avère pratique lorsque l'ordinateur est partagé. Vous empêcherez ainsi les autres utilisateurs de modifier vos paramètres ou d'installer un logiciel qui pourrait affecter le fonctionnement du PC.

Un deuxième compte peut se révéler pratique, même si vous êtes la seule personne à utiliser l'ordinateur. Un compte standard vous permettra d'empêcher qu'une action malencontreuse perturbe le fonctionnement du système. Lorsque vous souhaiterez installer un logiciel ou modifier des paramètres, il vous suffira simplement de vous connecter au compte administrateur.

Windows 10

1 Cliquez sur “Rechercher” et tapez “Autres utilisateurs”. Sélectionnez “Ajouter un autre utilisateur [...]”
2 Sélectionnez le type de compte à créer : un membre de la famille ou quelqu’un d’autre.

Créer un compte d’utilisateur



Pour un membre de la famille

S’il s’agit d’un membre de la famille, vous disposez en tant qu’administrateur d’un large panel de possibilités pour contrôler les activités de l’utilisateur. Cela peut s’avérer utile si vous désirez autoriser des enfants à accéder à l’ordinateur. Vous pourrez ainsi vérifier quelles applis ils utilisent et limiter les sites auxquels ils ont accès. Vous pourrez également limiter le temps d’écran afin qu’ils ne restent pas indéfiniment plantés devant l’ordinateur. Ces possibilités ne sont disponibles qu’avec un compte Microsoft.

D’autres personnes

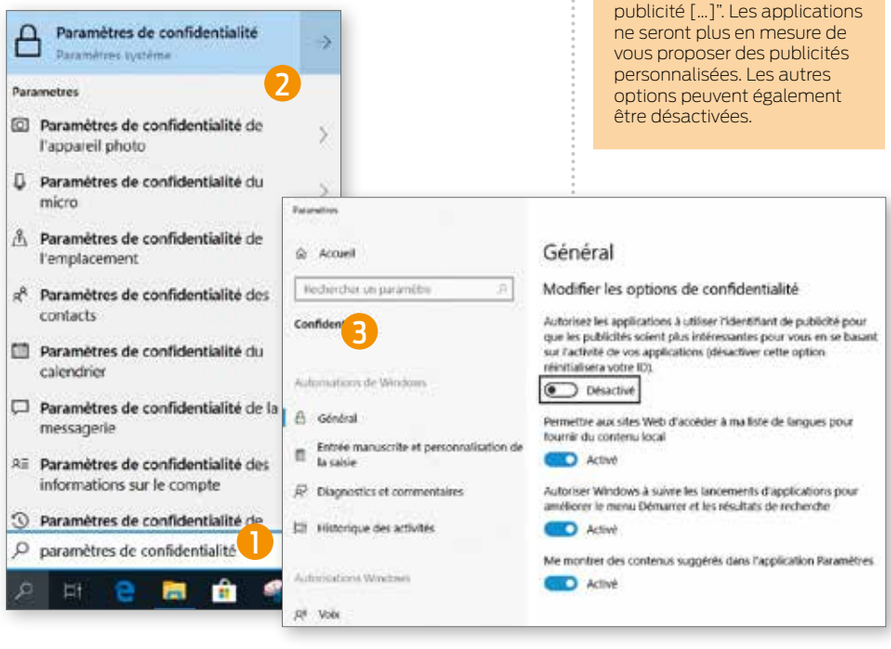
Vous pouvez également créer un compte invité au cas où un visiteur voudrait utiliser votre ordinateur pendant un certain temps. Pour cela, choisissez “Ajouter un autre utilisateur sur ce PC”. Encore une fois, Windows vous poussera à associer un compte Microsoft à ce nouveau compte, mais ce n’est pas nécessaire. Dans ce cas, optez pour “Je ne dispose pas des informations de connexion de cette personne” puis, sur la page suivante, sélectionnez “Ajouter un utilisateur sans compte Microsoft”. Enfin, choisissez un nom pour le compte invité (p. ex. “Invité”) et éventuellement un mot de passe.

1.3 TENEZ VOTRE CONFIDENTIALITÉ À L’ŒIL

Windows 10 ne bénéficie pas de la meilleure réputation en matière de confidentialité. Microsoft collecte en effet un grand nombre d’informations sur ses utilisateurs, bien plus que dans les versions précédentes de Windows. Il est heureusement possible d’y remédier.
Windows 10 dispose d’un menu de confidentialité. Cliquez sur Rechercher et tapez “Paramètres de confidentialité” pour y accéder. Il est recommandé de parcourir tous les sous-menus et de désactiver toutes les options de confidentialité, ou du moins en partie. Nous allons à présent aborder les principaux paramètres.

1.3a Les options de confidentialité générales

Si vous souhaitez modifier les options de confidentialité, vous accéderez d’abord à un écran qui vous permettra d’effectuer des réglages d’ordre général :



Confidentialité

1 Cliquez sur “Rechercher” et tapez “confidentialité”.
2 Cliquez sur “Paramètres de confidentialité”.
3 Sur l’écran “Modifier les options de confidentialité”, désactivez la première option, “Autorisez les applications à utiliser l’identifiant de publicité [...]”. Les applications ne seront plus en mesure de vous proposer des publicités personnalisées. Les autres options peuvent également être désactivées.