

GUIDE D'UTILISATION

**Bitdefender**® CONSUMER  
SOLUTIONS

# Password Manager





# Bitdefender Password Manager

## Guide de l'utilisateur

Date de publication : 06/09/2023  
Copyright © 2023 Bitdefender

## Mention légale

**Tous les droits sont réservés.** Aucune partie de ce livre ne peut être reproduite ou transmise sous quelque forme ou par quelque moyen que ce soit, électronique ou mécanique, y compris la photocopie, l'enregistrement ou par tout système de stockage et de récupération d'informations, sans l'autorisation écrite d'un représentant autorisé de Bitdefender. L'inclusion de brèves citations dans les critiques n'est possible qu'avec la mention de la source citée. Le contenu ne peut en aucun cas être modifié.

**Avertissement et clause de non-responsabilité.** Ce produit et sa documentation sont protégés par copyright. Les informations contenues dans ce document sont fournies « telles quelles », sans garantie. Bien que toutes les précautions aient été prises lors de la préparation de ce document, les auteurs n'assumeront aucune responsabilité envers toute personne ou entité en ce qui concerne toute perte ou dommage causé ou prétendument causé directement ou indirectement par les informations contenues dans ce travail.

Ce livre contient des liens vers des sites Web tiers qui ne sont pas sous le contrôle de Bitdefender. Par conséquent, Bitdefender n'est pas responsable du contenu de tout site lié. Si vous accédez à un site Web tiers répertorié dans ce document, vous le ferez à vos risques et périls. Bitdefender fournit ces liens uniquement à titre de commodité, et l'inclusion du lien n'implique pas que Bitdefender approuve ou accepte toute responsabilité quant au contenu du site tiers.

**Marques de commerce.** Des noms de marque peuvent apparaître dans ce livre. Toutes les marques déposées et non déposées dans ce document sont la propriété exclusive de leurs propriétaires respectifs et sont respectueusement reconnues.

Bitdefender®



# Table des matières

<b>À propos de ce guide .....</b>	<b>1</b>
Objectifs et destinataires .....	1
Comment utiliser ce guide .....	1
Conventions utilisées dans ce guide .....	1
Normes typographiques .....	1
Avertissement .....	2
Commentaires .....	2
<b>1. Qu'est-ce Bitdefender Password Managerque .....</b>	<b>4</b>
1.1. Sécurité et fonctionnement .....	4
1.2. Version d'essai et version payante de Password Manager .....	4
<b>2. Pour démarrer .....</b>	<b>5</b>
2.1. Configuration requise .....	5
2.1.1. Logiciels .....	6
2.2. Installation .....	6
2.2.1. Installation sur les appareils Windows et macOS .....	6
2.2.2. Installation sur les appareils Android .....	8
2.2.3. Installation sur les appareils iOS .....	10
<b>3. Forfait partagé .....</b>	<b>13</b>
3.1. Partager Bitdefender Password Manager avec plusieurs utilisateurs .....	13
<b>4. Importation et exportation de vos mots de passe .....</b>	<b>16</b>
4.1. Compatibilité .....	16
4.2. Importation des données dans Password Manager .....	17
4.3. Exportation des données depuis Password Manager .....	19
<b>5. Caractéristiques et fonctionnalités .....</b>	<b>21</b>
5.1. Gestion des mots de passe .....	21
5.1.1. Générateur de mots de passe .....	21
5.1.2. Capture des mots de passe .....	22
5.1.3. Remplissage automatique intelligent .....	22
5.1.4. Rapport de sécurité .....	22
5.1.5. Synchronisation sur de multiples plateformes .....	23
5.1.6. Suppression des mots de passe .....	23
5.2. Gestion des comptes .....	23
5.2.1. Authentification .....	23
5.2.2. Réinitialisation du mot de passe principal .....	24
5.3. Autres fonctionnalités .....	26
5.3.1. Gestion des identités .....	26
5.3.2. Gestion des cartes bancaires .....	26
5.3.3. Secure Me .....	27



5.3.4. Notes .....	27
<b>6. Foire aux questions .....</b>	<b>29</b>
<b>7. Obtenir de l'aide .....</b>	<b>33</b>
7.1. Demander de l'aide .....	33
7.2. Ressources En Ligne .....	33
7.2.1. Centre de support Bitdefender .....	33
7.2.2. Communauté des experts Bitdefender .....	34
7.2.3. Bitdefender Cyberpedia .....	34
7.3. Pour nous joindre .....	35
7.3.1. Distributeurs locaux .....	35
<b>Glossaire .....</b>	<b>36</b>



## À PROPOS DE CE GUIDE

### Objectifs et destinataires

Ce guide s'adresse à tous les utilisateurs de Bitdefender sur les systèmes d'exploitation compatibles (Windows, MacOS, Android et iOS) qui ont choisi Bitdefender Password Manager comme outil de gestion de leurs mots de passe. Il se veut accessible à tous, il n'est pas nécessaire de bien s'y connaître en informatique pour le comprendre.

Ce guide présente en détail toutes les caractéristiques et fonctionnalités de notre gestionnaire de mots de passe ultra-sécurisé, pour vous aider à en tirer le meilleur.

Nous vous souhaitons un apprentissage agréable et utile.

### Comment utiliser ce guide

Ce guide couvre plusieurs thèmes essentiels :

[Pour démarrer \(page 5\)](#)

Installation et démarrage de Bitdefender Password Manager.

[Caractéristiques et fonctionnalités \(page 21\)](#)

Utilisation de Bitdefender Password Manager et de toutes ses fonctionnalités.

[Obtenir de l'aide \(page 33\)](#)

Où chercher et à qui demander de l'aide en cas d'imprévu

### Conventions utilisées dans ce guide

#### Normes typographiques

Plusieurs styles de texte sont utilisés dans ce guide pour une lisibilité améliorée. Leur aspect et signification sont présentés dans la liste ci-dessous.



Style	Description
sample syntax	Les exemples de syntaxe sont écrits dans une police à espacement fixe.
<a href="https://www.bitdefender.com">https://www.bitdefender.com</a>	Les liens URL renvoient vers un emplacement externe comme un serveur http ou ftp.
<a href="mailto:documentation@bitdefender.com">documentation@bitdefender.com</a>	Les adresses email sont insérées dans le texte pour plus d'informations sur les contacts.
<a href="#">À propos de ce guide (page 1)</a>	Ceci représente un lien interne vers un emplacement à l'intérieur de ce document.
Nom de fichier	Les noms de fichiers et de répertoires sont écrits dans une police à espacement fixe.
<b>Option</b>	Toutes les options du produit sont écrites en caractères <b>gras</b> .
<b>Mot-clé</b>	Les mots-clés et les expressions importantes sont mis en évidence à l'aide de caractères <b>gras</b> .

## Avertissement

Les avertissements sont des notes mises en évidence pour attirer votre attention sur des informations complémentaires relatives au paragraphe dans lequel elles se trouvent.



### Note

Les notes sont de courtes observations. Vous pouvez les survoler, mais elles comportent des informations intéressantes, comme des précisions sur des fonctions spécifiques ou un lien vers un thème proche.



### Important

Le texte précédé de cette icône requiert votre attention et nous vous recommandons de ne pas l'ignorer. Il fournit habituellement des informations non essentielles mais utiles.



### Attention

Le texte précédé de cette icône contient des informations essentielles que vous devez lire attentivement. Si vous suivez les indications, tout se passera bien. Assurez-vous de bien les comprendre, car elles décrivent des procédures dangereuses.

## Commentaires

Aidez-nous à améliorer ce livret ! Nous avons testé et vérifié toutes les informations mais n'hésitez pas à nous écrire pour nous signaler



d'éventuelles erreurs ou des améliorations que nous pourrions y apporter pour vous fournir la meilleure documentation possible.

Écrivez-nous à l'adresse [documentation@bitdefender.com](mailto:documentation@bitdefender.com). Merci de bien vouloir rédiger en anglais vos e-mails concernant cette documentation afin que nous puissions les traiter efficacement.



# 1. QU'EST-CE BITDEFENDER PASSWORD MANAGERQUE

Bitdefender Password Manager est un service multiplateforme qui aide les utilisateurs à stocker et à organiser tous leurs mots de passe en ligne. Il dispose des algorithmes de chiffrement les plus puissants à ce jour, pour une sécurité numérique optimale. Il se présente sous la forme d'une extension de navigateur et d'une application mobile permettant de gérer l'identité, les mots de passe et toutes les informations sensibles - notamment bancaires - sur tous les appareils.

Bitdefender Password Manager peut enregistrer, saisir, générer et gérer automatiquement vos mots de passe pour tous les sites Web et services en ligne que vous utilisez à l'aide d'un mot de passe principal, ce qui facilite grandement la gestion globale de votre identité numérique.

## 1.1. Sécurité et fonctionnement

Pour offrir une sécurité de pointe aux utilisateurs, le logiciel Bitdefender Password Manager est équipé des derniers algorithmes de chiffrement, dont les protocoles AES-256-CCM, SHA512, BCRYPT, HTTPS et WSS pour la transmission de données. Toutes les données sont chiffrées et déchiffrées localement. Ainsi, le titulaire du compte est le seul à avoir accès aux informations stockées et au mot de passe principal utilisé pour consulter et utiliser les données en question.

## 1.2. Version d'essai et version payante de Password Manager

La version d'essai de Bitdefender Password Manager fonctionne exactement comme la version payante, mais elle expirera 90 jours après son activation.



### Note

Remarque : la version payante peut être achetée indépendamment, mais elle est incluse dans les abonnements à Bitdefender Premium Security et Bitdefender Ultimate Security.





## 2. POUR DÉMARRER

### 2.1. Configuration requise

Vous pouvez utiliser la dernière version de Bitdefender Password Manager uniquement sur les appareils fonctionnant avec les systèmes d'exploitation suivants :

○ **Pour les utilisateurs d'appareils Windows :**

- Windows 7 avec Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

○ **Pour les utilisateurs d'appareils macOS :**

- Système d'exploitation macOS 10.14 (Mojave) ou ultérieur



**Note**

Remarque : les performances du système peuvent être réduites sur les appareils équipés d'anciennes générations de processeurs.

○ **Pour les utilisateurs d'appareils iOS :**

- Système d'exploitation iOS 11.0 ou ultérieur

○ **Pour les utilisateurs d'appareils Android :**

- Système d'exploitation Android 5.1 ou ultérieur



**Note**

- Le déverrouillage par empreinte digitale est disponible sur **Android 6.0** et les systèmes d'exploitation ultérieurs.
- La saisie automatique est disponible sur **Android 8.0** et les systèmes d'exploitation ultérieurs, elle est compatible avec les appareils iPhone, iPad et iPod touch.



## 2.1.1. Logiciels

Pour que vous puissiez utiliser Bitdefender Password Manager et l'ensemble de ses fonctionnalités, vos appareils Windows ou macOS doivent disposer de la configuration logicielle suivante :

- **Microsoft Edge** (basé sur Chromium 80 ou une version ultérieure)
- **Mozilla Firefox** (version 65 ou ultérieure)
- **Google Chrome** (version 72 ou ultérieure)
- **Safari** (version 12 ou ultérieure)



### Note

Ces recommandations ne valent pas pour Android et iOS.



### Avertissement

Si vos appareils ne disposent pas de la configuration requise, Bitdefender Password Manager ne pourra pas être installé ou ne fonctionnera pas correctement.

## 2.2. Installation

Ce chapitre explique comment installer Bitdefender Password Manager sur les navigateurs web des ordinateurs Windows et macOS, ainsi que sur les appareils mobiles Android ou iOS.



### Important

Avant de procéder à l'installation, assurez-vous que vous disposez d'un abonnement à Password Manager en consultant votre compte **Bitdefender Central**, pour que cette extension de navigateur soit bien rattachée à votre compte.

Les abonnements actifs figurent dans la section **Mes abonnements** de Bitdefender Central.

### 2.2.1. Installation sur les appareils Windows et macOS

Contrairement à la plupart des applications et des logiciels qui doivent être installés et configurés directement sur ces appareils Bitdefender Password Manager se présente sous la forme d'une extension de navigateur - aussi appelée « module complémentaire » - qui peut facilement être installée et activée sur le navigateur de votre choix.



Actuellement, les navigateurs compatibles avec le produit sont les suivants : **Google Chrome, Mozilla Firefox, Microsoft Edge** et **Safari**.

1. Rendez-vous sur <https://central.bitdefender.com/> et connectez-vous à votre compte.  
Si vous n'avez pas encore de compte, cliquez sur **CRÉER UN COMPTE**, puis saisissez votre nom complet, une adresse e-mail et un mot de passe.
2. Sélectionnez **Mes appareils**, dans la barre latérale à gauche de l'écran.
3. Dans la section **Mes appareils**, cliquez sur **+ Ajouter un appareil**.
4. Une nouvelle fenêtre s'ouvre. Sélectionnez **Password Manager**.
5. Cliquez sur **Cet appareil**.  
Si vous souhaitez installer le produit sur un autre appareil, cliquez sur **Autres appareils**. Vous pouvez ensuite envoyer un lien de téléchargement à l'appareil concerné ou copier l'URL d'installation.
6. Choisissez le navigateur sur lequel vous souhaitez installer l'extension Password Manager.
7. Chaque bouton renvoie au catalogue des extensions disponibles pour le navigateur concerné. À partir de là, suivez les instructions qui s'affichent à l'écran (voir ci-dessous).

### **Microsoft Edge**

- Cliquez sur le bouton **Obtenir**
- Cliquez sur **Ajouter l'extension** dans la fenêtre qui s'affiche

### **Google Chrome**

- Cliquez sur le bouton **Ajouter à Chrome**
- Dans la fenêtre de confirmation, cliquez sur **Ajouter l'extension**

### **Mozilla Firefox**

- Cliquez sur le bouton **Ajouter à Firefox**
- Cliquez sur le bouton **Ajouter** en haut à droite de l'écran

### **Safari**

- Cliquez sur le bouton **Obtenir**, puis sur **Installer**



- Ouvrez Safari et sélectionnez **Préférences** dans le menu en haut de l'écran
- Dans la fenêtre Préférences, cliquez sur l'onglet **Extensions**
- Cochez la case de Password Manager pour l'activer

Une fois ces étapes terminées, définissez un mot de passe principal fort puis cliquez sur le bouton **Enregistrer le mot de passe principal** après avoir lu et accepté les **Conditions générales**.



### Important

Ce mot de passe principal permet d'accéder à l'ensemble des mots de passe, notes et informations de carte bancaire conservés dans Bitdefender Password Manager. Il s'agit en quelque sorte de la clé du produit.



### Avertissement

Immédiatement après la création de votre mot de passe principal, vous recevrez une **clé de récupération à 24 chiffres**. **Notez-la et conservez-la en lieu sûr**. Si jamais **vous oubliez le mot de passe principal** associé à votre compte, cette clé est le seul moyen de récupérer vos mots de passe enregistrés dans Password Manager.

- Ensuite, cliquez sur **Fermer**.

## 2.2.2. Installation sur les appareils Android


Pour installer Bitdefender Password Manager sur des téléphones ou des tablettes Android, le plus simple est de télécharger l'application directement depuis Google Play.



L'installation peut également se faire depuis votre compte **Bitdefender Central** :

1. Sur votre appareil mobile Android, connectez-vous à votre compte Bitdefender Central en vous rendant à l'adresse <https://login.bitdefender.com/central/login>.
2. Sélectionner **Mes appareils** dans la barre latérale gauche de l'écran.



3. Dans le **Mes appareils** section, continuez en cliquant sur **+ Ajouter un appareil**.
4. Cette action fera apparaître une nouvelle fenêtre. Choisir **Gestionnaire de mots de passe** dans l'écran de sélection.
5. Choisir **Cet appareil**.  
Si vous souhaitez installer le produit sur un autre appareil, cliquez sur **Autres appareils**. Vous pouvez ensuite envoyer un lien de téléchargement à l'appareil concerné ou copier l'URL d'installation.
6. **Google Play** s'ouvre. Appuyez sur **Installer** pour télécharger Bitdefender Password Manager sur Android.
7. Une fois le téléchargement terminé, ouvrez l'application  Password Manager.
8. Si la connexion n'est pas automatiquement établie, connectez-vous à votre compte en utilisant votre nom d'utilisateur et votre mot de passe.  
Une fois que vous avez suivi ces étapes, définissez un mot de passe principal fort, puis appuyez sur la **Enregistrer le mot de passe principal** bouton après avoir lu et accepté le **Termes et conditions**.



### Important

Notez que vous aurez besoin de ce mot de passe principal pour déverrouiller tous les mots de passe, les informations de carte de crédit et les notes enregistrées dans Bitdefender Password Manager. C'est essentiellement la clé qui permet au propriétaire d'utiliser ce produit.



### Avertissement

Lors de la création du mot de passe principal, vous recevrez un **Clé de récupération à 24 chiffres**. **Notez votre clé de récupération dans un endroit sûr et ne la perdez pas**. Cette clé est le seul moyen d'accéder à vos mots de passe enregistrés dans Password Manager au cas où vous **oubliez le mot de passe principal** précédemment configuré pour votre compte.

Vous pouvez appuyer sur **Fermer** lorsque vous avez terminé.

9. Créez un **code PIN à 4 chiffres**. Il vous permettra de ne pas avoir à saisir de nouveau le mot de passe principal que vous aurez défini



si vous réutilisez Password Manager après avoir essayé une autre application.

- 10 Appuyez sur **Remplissage automatique** pour configurer les paramètres du remplissage automatique sur Android.



### Note

Si vous ignorez cette étape, vous pouvez activer et personnaliser ces paramètres ultérieurement en suivant les instructions disponibles sur [Remplissage automatique intelligent \(page 22\)](#).

- 11 Une liste d'applications de remplissage automatique des mots de passe s'affiche.

Sélectionnez **Password Manager**. Il vous est alors demandé de confirmer que vous faites confiance à cette application.

Appuyez sur **OK**.

- 12 Saisissez le code PIN que vous avez défini à l'**étape 9** pour confirmer votre choix.

L'application est désormais installée sur votre appareil Android.

### 2.2.3. Installation sur les appareils iOS

Pour installer Bitdefender Password Manager sur des appareils iOS and iPadOS, le plus simple est de télécharger l'application directement depuis l'App Store Apple.



L'installation de l'application Bitdefender Password Manager peut également être effectuée via votre [Centrale Bitdefender](#) compte:

1. Sur votre iPhone ou votre iPad, connectez-vous à votre compte Bitdefender Central en vous rendant à l'adresse <https://login.bitdefender.com/central/login>.
2. Sélectionner **Mes appareils** dans la barre latérale gauche de l'écran.
3. Dans le **Mes appareils** section, continuez en cliquant sur **+ Ajouter un appareil**.
4. Cette action fera apparaître une nouvelle fenêtre. Choisir **Gestionnaire de mots de passe** dans l'écran de sélection.



### 5. Choisir **Cet appareil**.

Si vous cherchez à installer sur un autre appareil, sélectionnez **Autres appareils**. Vous pouvez ensuite envoyer un lien de téléchargement par e-mail à l'appareil concerné ou copier directement l'URL de l'installation.

### 6. L'**App Store** s'ouvre. Appuyez sur l'icône représentant un nuage et une flèche orientée vers le bas pour télécharger Bitdefender Password Manager pour iOS.

### 7. Une fois l'application installée, ouvrez-la et cochez la case qui apparaît à l'écran. Sélectionnez **Continuer** après avoir lu et accepté les dispositions du **contrat d'abonnement**.

### 8. Si vous n'êtes pas automatiquement connecté à votre compte, connectez-vous en utilisant votre nom d'utilisateur et votre mot de passe.

Une fois que vous avez suivi ces étapes, définissez un mot de passe principal fort, puis appuyez sur la **Enregistrer le mot de passe principal** bouton après avoir lu et accepté le **Termes et conditions**.



#### Important

Notez que vous aurez besoin de ce mot de passe principal pour déverrouiller tous les mots de passe, les informations de carte de crédit et les notes enregistrées dans Bitdefender Password Manager. C'est essentiellement la clé qui permet au propriétaire d'utiliser ce produit.



#### Avertissement

Lors de la création du mot de passe principal, vous recevrez un **Clé de récupération à 24 chiffres**. [Notez votre clé de récupération dans un endroit sûr et ne la perdez pas](#). Cette clé est le seul moyen d'accéder à vos mots de passe enregistrés dans Password Manager au cas où vous **oubliez le mot de passe principal** précédemment configuré pour votre compte.

Vous pouvez appuyer sur **Fermer** lorsque vous avez terminé.

### 9. Créer un **NIP à 4 chiffres**, ainsi, si vous passez à une autre application, puis revenez à Password Manager, vous n'aurez pas à ressaisir le mot de passe principal que vous avez configuré précédemment. Si



disponible, vous pouvez également activer la reconnaissance faciale ou l'authentification par empreinte digitale.

L'application est désormais installée sur votre appareil iOS / iPadOS.





## 3. FORFAIT PARTAGÉ

**Forfait partagé Bitdefender Password Manager** permet à plusieurs utilisateurs d'accéder et d'utiliser le même abonnement. Il fournit une approche centralisée de l'accès, de l'administration et du support aux logiciels.

- La personne en charge du plan d'abonnement partagé, appelé Plan Manager, peut partager le service entre les membres.
- Chaque membre obtient son propre **Bitdefender Central** compte lié à son adresse e-mail et accès au service Bitdefender Password Manager.

### 3.1. Partager Bitdefender Password Manager avec plusieurs utilisateurs

#### Inviter des membres

Pour ajouter un ou plusieurs utilisateurs à l'abonnement partagé, le gestionnaire du forfait doit suivre ces étapes :

1. Connectez-vous à votre compte Bitdefender Central à l'adresse <https://central.bitdefender.com/>.
2. Allez dans le menu **Mes abonnements** situé sur le côté gauche de la page.
3. Choisissez **Inviter un membre** dans le panneau **Plan partagé de Bitdefender Password Manager**.
4. Saisissez l'e-mail de chaque personne avec laquelle vous souhaitez partager votre abonnement, puis cliquez sur **Envoyer**. Un maximum de 3 membres peut être ajouté en même temps.
5. Les instructions d'installation sont envoyées immédiatement par e-mail aux nouveaux membres. Cliquez sur **Fermer** pour quitter la fenêtre de confirmation.



## Note

Les membres ont 24 heures pour accepter votre invitation une fois qu'elle leur a été envoyée par courrier électronique.

- Les membres invités apparaîtront avec le statut « Invité ».
- Vous les verrez comme membres « actifs » après avoir accepté l'invitation. Vous êtes également averti par email de chaque invitation acceptée.

## Supprimer des membres

L'accès au plan partagé de Bitdefender Password Manager est perdu pour les membres qui sont retirés. Lorsque le gestionnaire du plan décide de supprimer un membre de l'abonnement, ce dernier reçoit une notification par e-mail. Pendant les 30 jours suivants, l'ancien membre passe à une version d'essai de 30 jours de Bitdefender Password Manager avec toutes les fonctionnalités. Le service sera ensuite désactivé.

Le gestionnaire du plan peut éliminer des utilisateurs du plan partagé de la manière suivante:

1. Connectez-vous à votre compte Bitdefender Central à l'adresse <https://central.bitdefender.com/>.
2. Allez dans le menu **Mes abonnements** situé sur le côté gauche de la page.
3. Dans le panneau **Plan partagé de Bitdefender Password Manager**, cliquez sur **Gérer**, puis choisissez **Modifier les membres** dans le menu.
4. Cliquez sur le bouton **Supprimer** pour retirer un membre du plan partagé.
5. Choisissez **Oui, supprimer le membre** puis cliquez sur le bouton **Terminer l'édition** pour que les modifications prennent effet.



## Note

Lorsqu'un membre est supprimé du plan partagé, son statut passe à **En attente de suppression** jusqu'à ce qu'il soit complètement éliminé.

## Accepter une invitation

Vous recevrez un e-mail lorsque quelqu'un vous invitera à devenir membre du forfait partagé Bitdefender Password Manager. Vous disposez



de 24 heures pour accepter une invitation une fois qu'elle vous est envoyée.

Pour accepter l'invitation et accéder aux fonctionnalités du gestionnaire de mots de passe, l'utilisateur doit suivre ces étapes :

1. Ouvrez l'e-mail que vous avez reçu intitulé **[Commencez à utiliser votre abonnement Bitdefender en tant que membre]** et cliquez sur le bouton **ACTIVER DANS CENTRAL**.
2. La page Bitdefender Central s'ouvrira alors dans votre navigateur.
  - Si vous avez déjà un compte utilisateur Bitdefender associé à l'email où l'invitation a été envoyée, **connectez-vous** pour réclamer votre abonnement partagé.
  - Si vous n'avez pas de compte utilisateur Bitdefender, cliquez sur **Créer un compte** et inscrivez-vous avec l'email où l'invitation a été envoyée pour réclamer votre abonnement partagé.
    - Saisissez votre nom complet
    - Saisissez votre adresse e-mail
    - Entrez votre mot de passe
    - Cliquez sur le bouton Créer un compte et vous serez signé.
3. Une fois connecté, cliquez sur **Démarrer** sur l'écran de bienvenue qui vous informe que votre abonnement à Bitdefender Password Manager est maintenant actif.
4. Suivez les étapes à l'écran également décrites dans [Installation \(page 6\)](#).



### Note

L'e-mail du gestionnaire de forfait est affiché dans votre compte Bitdefender Central en haut du menu Gestionnaire de mots de passe et sur la carte d'abonnement, sous Mes abonnements.

Si vous avez besoin d'aide avec le forfait partagé, veuillez les contacter.



## 4. IMPORTATION ET EXPORTATION DE VOS MOTS DE PASSE

Bitdefender Password Manager est conçu de manière à faciliter la communication avec des sources, plateforme et outils logiciels extérieurs et le transfert de données qui en proviennent. Il permet donc d'importer et d'exporter des mots de passe très simplement.

### 4.1. Compatibilité

Bitdefender Password Manager peut sans difficulté transférer des données provenant des applications suivantes :

- 1Password**
- Bitwarden**
- Bitdefender Password Manager**
- ByePass**
- Chrome browser**
- Claro**
- Dashlane**
- Edge browser**
- ESET Password Manager v2**
- ESET Password Manager v3**
- StickyPassword**
- Watchguard**
- Firefox browser**
- Gestor de contraseñas – Claro**
- Gestor de contraseñas – SIT**
- Gestor de contraseñas – Telnor**
- KeePass 2.x**
- LastPass**
- Panda Dome Passwords**



- PassWatch
- Saferpass
- SFR Cybersécurité
- SIT
- F-Secure
- Telnor



## Note

Si le nom du navigateur ou du gestionnaire de mots de passe dont vous voulez exporter les données ne figure pas sur cette liste, consultez le guide en ligne pour savoir comment préparer un fichier CSV qui vous permettra d'importer les données des outils non pris en charge dans **Bitdefender Password Manager** : <https://www.bitdefender.fr/consumer/support/answer/11039/>

Ce transfert de données entre Bitdefender Password Manager et d'autres logiciels de gestion de comptes peut se faire à l'aide de fichiers aux formats suivants :

**CSV, JSON, XML, TXT, 1pif et FSK.**

## 4.2. Importation des données dans Password Manager

Bitdefender Password Manager vous permet d'importer facilement des mots de passe provenant de navigateurs ou d'autres gestionnaires. Si vous utilisez déjà un autre service de gestion des mots de passe, vous y avez sans doute stocké beaucoup d'informations (noms d'utilisateur, mots de passe et autres éléments d'identification requis pour accéder à vos différents comptes).

Maintenant que vous avez choisi Bitdefender Password Manager, vous devez y importer vos données précédemment enregistrées.

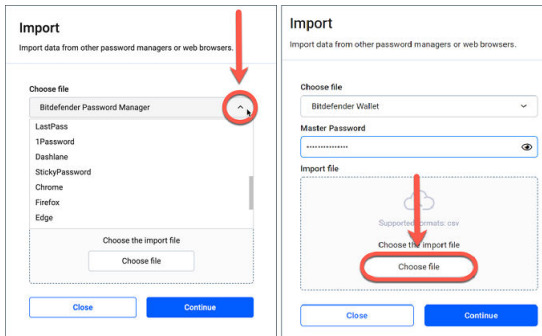
Voici comment procéder pour importer les informations stockées par d'autres applications et navigateurs dans Bitdefender Password Manager, **quel que soit le système d'exploitation** sur lequel vous avez installé ce produit :

1. Cliquez sur l'icône Password Manager dans votre navigateur (sur Windows ou macOS) ou lancez l'application Password Manager (sur



Android ou iOS). Si le système vous le demande, saisissez votre **mot de passe principal**.

2. Ouvrez le menu Password Manager ☰ pour développer la barre latérale gauche, puis cliquez sur ⚙️ **Paramètres**.
3. Faites défiler la liste jusqu'à la section **Données**, puis cliquez sur **Importer des données**.
4. Ouvrez le menu défilant pour sélectionner le nom du gestionnaire de mots de passe ou du navigateur qui contient vos données. Saisissez votre **mot de passe principal** dans le champ correspondant, puis cliquez sur **Choisir un fichier**.



5. Parcourez vos dossiers jusqu'à l'emplacement où se trouve le fichier contenant vos noms d'utilisateur et vos mots de passe exportés depuis un navigateur ou un autre gestionnaire de mots de passe, puis cliquez sur **Continuer**.

Une fois importés, vos mots de passe seront accessibles sur tous les appareils sur lesquels l'application ou l'extension de navigateur Bitdefender Password Manager est installée.



## 4.3. Exportation des données depuis Password Manager


Bitdefender Password Manager vous permet d'exporter facilement les mots de passe que vous avez sauvegardés (identifiants de comptes, notes sécurisées, etc.) dans un fichier CSV (fichier de valeurs séparées par des virgules) ou dans un fichier chiffré si jamais vous souhaitez passer à un autre service de gestion des mots de passe. Ainsi, la transition se fera sans difficulté.



### Important

Les fichiers CSV ne sont **pas** chiffrés, les noms d'utilisateur et les mots de passe y apparaissent en texte brut. Cela signifie que ces informations confidentielles peuvent être consultées par toute personne ayant accès à votre appareil. Par conséquent, nous vous recommandons de suivre les instructions ci-dessous sur un appareil de confiance.

Voici comment procéder pour exporter vos données depuis Bitdefender Password Manager :

1. Cliquez sur l'icône Password Manager dans votre navigateur Web (sous Windows ou macOS) ou lancez l'application Password Manager (sous Android ou iOS). Si vous y êtes invité, entrez votre [Mot de passe maître](#).
2. Ouvrez le menu Password Manager pour développer la barre latérale gauche, puis cliquez sur  **Paramètres**.
3. Faites défiler la liste jusqu'à la section **Données**, puis cliquez sur **Exporter des données**.
4. Deux options vous sont alors proposées :
  - CSV**
  - Fichier protégé par mot de passe**

Faites votre choix, puis saisissez votre mot de passe principal et cliquez sur **Exporter des données**.



### Note

Si vous avez choisi l'option Fichier protégé par mot de passe, vous devez à ce stade chiffrer les données à l'aide d'un mot de passe, pour que personne d'autre que vous ne puisse y accéder si nécessaire.

5. Le navigateur/l'application enregistre un fichier nommé Bitdefender Password Manager\_exported\_data\_current-date dans le dossier de téléchargement de votre système. Il contient toutes les données stockées dans Bitdefender Password Manager.

Une fois vos données exportées, vous pouvez les importer dans le gestionnaire de mots de passe de votre choix.





## 5. CARACTÉRISTIQUES ET FONCTIONNALITÉS


Ce chapitre présente en détail toutes les caractéristiques et fonctionnalités de Bitdefender Password Manager, et vous explique comment les utiliser le plus efficacement possible.

### 5.1. Gestion des mots de passe

#### 5.1.1. Générateur de mots de passe


Afin de préserver votre sécurité en ligne, la règle d'or est d'utiliser systématiquement des mots de passe générés aléatoirement pour chaque service qui nécessite la création d'un compte. La réutilisation du même mot de passe sur de multiples plateformes est le principal facteur qui augmente le risque de prise de contrôle des comptes, mais aussi de fuite des données et d'usurpation d'identité.

Cette fonctionnalité permet aux utilisateurs de générer des mots de passe forts, complexes et uniques pour chaque nouveau compte créé en ligne. Ils n'ont donc plus besoin de les imaginer ou de veiller à ne pas les réutiliser sur de multiples comptes.

Le  **générateur de mots de passe** est accessible depuis l'onglet situé en haut de l'interface de Password Manager.

Il permet de créer des mots de passe comprenant **entre 4 et 32 caractères**.

Vous pouvez préciser les types de caractères à inclure ou exclure des mots de passe générés aléatoirement en cochant ou décochant les cases correspondantes. (**minuscules, majuscules, chiffres, caractères spéciaux**).

Si le mot de passe proposé ne vous convient pas, appuyez sur le bouton  qui se trouve à droite de celui-ci pour que le système en crée un autre.

Pour utiliser le mot de passe affiché, cliquez sur **Utiliser ce mot de passe**. La séquence de caractères est alors enregistrée dans votre presse-papiers.



## Note





Vos mots de passe générés précédemment sont temporairement stockés dans l'historique des mots de passe. Vous pouvez y accéder en cliquant sur le bouton **Historique des mots de passe**.

## 5.1.2. Capture des mots de passe

Grâce à cette fonctionnalité, Password Manager vous invite à stocker tous vos nouveaux mots de passe immédiatement après leur création, pour qu'ils bénéficient tout de suite de l'environnement ultra-sécurisé garanti par Bitdefender.

## 5.1.3. Remplissage automatique intelligent

Bitdefender Password Manager peut être configuré de manière à saisir automatiquement vos identifiants, et surtout vos mots de passe. Des algorithmes propriétaires peuvent détecter et préremplir les champs appropriés sur les sites que vous avez déjà visités, ce qui vous permet de gagner du temps à chaque connexion.

1. Sur Windows ou macOS, cliquez sur l'icône  **Password Manager** dans votre navigateur.  
Sur Android ou iOS, lancez l'application  **Password Manager**.  
Si le système vous le demande, saisissez votre **mot de passe principal**.
2. Ouvrez le menu Password Manager  pour développer la barre latérale gauche, puis cliquez sur  **Paramètres**.
3. Cliquez sur **Paramètres de l'appareil**.
4. Dans la fenêtre qui s'affiche, un bouton est réglé sur **Désactiver le remplissage automatique** ou **Activer le remplissage automatique**. Ce paramètre définit le fonctionnement de l'option Remplissage automatique intelligent.

## 5.1.4. Rapport de sécurité

L'outil Rapport de sécurité permet de générer un rapport portant sur plusieurs fonctionnalités conçues pour renforcer votre sécurité numérique. Ce rapport indique notamment si certains de vos mots de passe nécessitent votre attention en évaluant leur niveau de sécurité. Les



mots de passe en double sont détectés et signalés. Il vous est suggéré de les changer pour éviter de recycler les mêmes mots de passe sur différents comptes.

Le rapport vous aide à faire le point sur votre discipline en matière de mots de passe (mots de passe en double, mots de passe trop faibles, mots de passe et adresses e-mail déjà exposés, etc.)

Il y parvient en comparant la liste des hachages des pages web stockés localement sur votre appareil pour vérifier si certains d'entre eux correspondent à vos mots de passe. Si une correspondance est détectée, vous recevrez une notification vous encourageant à changer vos mots de passe et vos autres informations de connexion.

Pour consulter le **rapport de sécurité**, ouvrez l'interface Password Manager et cliquez sur l'icône correspondante  sur la barre supérieure.

### 5.1.5. Synchronisation sur de multiples plateformes



Une fois vos mots de passe stockés en toute sécurité dans Bitdefender Password Manager, vous pouvez les utiliser sur tous vos appareils Windows, Mac, Android ou iOS avec les navigateurs Chrome, Safari, Firefox Edge, ainsi que sur les applications mobiles.



#### Note

Bitdefender Password Manager est aussi équipé d'un **mode hors ligne** qui vous permet d'accéder à vos mots de passe partout et à tout moment, même sans connexion Internet.

### 5.1.6. Suppression des mots de passe

Pour supprimer un mot de passe enregistré, cliquez sur l'icône  Modifier à côté du mot de passe que vous souhaitez supprimer, dans l'onglet  **Comptes**. Faites défiler la page vers le bas puis cliquez sur **Supprimer**. Il vous est alors demandé de confirmer que vous voulez vraiment supprimer le compte. Pour confirmer votre choix cliquez sur **Supprimer**.

## 5.2. Gestion des comptes

### 5.2.1. Authentification

Dans Bitdefender Password Manager, l'authentification se fait à l'aide du **code PIN** défini lors de l'installation du produit. (Remarque : la fonction



**Verrouillage automatique** verrouille le gestionnaire de mots de passe ou déconnecte le produit après une période d'inactivité du navigateur ou au moment de la fermeture de l'application mobile).

Si votre appareil le permet, vous pouvez aussi utiliser des moyens d'identification biométrique, comme **la reconnaissance de l'empreinte digitale** ou **la reconnaissance faciale**.

Pour **activer ou désactiver** l'authentification biométrique :

1. Sous Windows ou macOS, cliquez sur le  **Password Manager** icône dans votre navigateur Web.  
Sur Android ou iOS, lancez le  **Password Manager** application.  
Si vous y êtes invité, entrez votre **Mot de passe maître**.
2. Ouvrez le menu du gestionnaire de mots de passe  pour développer la barre latérale sur la gauche et cliquez sur le  **Paramètres** élément du menu.
3. Cliquer sur **Réglages de l'appareil**.
4. Dans la fenêtre qui s'affiche, un bouton est réglé sur **Désactiver l'authentification biométrique** ou **Activer l'authentification biométrique**. Ce paramètre définit le fonctionnement de l'option Authentification biométrique.


### 5.2.2. Réinitialisation du mot de passe principal



#### Important

L'option **Modifier le mot de passe principal** n'est pas disponible sur les appareils mobiles. Le seul moyen de modifier ou de récupérer le mot de passe principal est de passer par l'extension Bitdefender Password Manager sur votre navigateur depuis un ordinateur Windows ou un appareil macOS.



Voici comment modifier votre **mot de passe principal** par mesure de précaution dans Bitdefender Password Manager :

1. Une fois l'extension installée, cliquez sur l'icône  **Password Manager** dans la barre d'outils de votre navigateur.
2. Saisissez votre mot de passe principal actuel pour déverrouiller le coffre-fort.



## Important

Si vous avez oublié votre mot de passe principal actuel, cliquez sur le bouton **J'ai oublié mon mot de passe**. Saisissez la **clé de récupération à 24 chiffres** qui vous a été fournie lors de la configuration initiale de Bitdefender Password Manager. **Si vous avez oublié ou perdu le mot de passe principal et la clé de récupération**, en dernier ressort, **contactez un représentant Bitdefender qui vous aidera à réinitialiser votre compte**. Cette opération **effacera toutes les données et tous les mots de passe enregistrés** dans Bitdefender Password Manager.

- Ouvrez le menu du gestionnaire de mots de passe  pour développer la barre latérale sur la gauche et cliquez sur le  **Paramètres** élément du menu.
- Cliquez sur le bouton **Mon compte** dans la section **Compte**.
- Une fenêtre contenant des informations sur votre abonnement à Password Manager s'affiche.  
Cliquez sur le bouton **Modifier le mot de passe principal**.
- Une nouvelle fenêtre s'ouvre, sur laquelle vous pouvez définir un nouveau mot de passe principal. Saisissez le mot de passe principal actuel, puis le nouveau. Celui-ci doit contenir au moins 8 caractères, dont au moins une minuscule, une majuscule et un chiffre.
- Ensuite, cliquez sur le bouton **Modifier**.
- Patiencez quelques instants pendant que Bitdefender réinitialise le mot de passe principal.  
Ne fermez pas votre navigateur web !
- Notez la nouvelle **clé de récupération à 24 chiffres** et conservez-la en lieu sûr. **Ne la perdez pas**. Si jamais vous oubliez le mot de passe principal, cette clé est le seul moyen de récupérer vos mots de passe enregistrés dans Password Manager.  
Une fois cette opération terminée, cliquez sur **Fermer**.
- Bitdefender Password Manager est alors déconnecté.
  - Pour déverrouiller le coffre-fort, utilisez le nouveau mot de passe principal que vous venez de définir.







## 5.3. Autres fonctionnalités

### 5.3.1. Gestion des identités

Cette fonctionnalité permet aux utilisateurs de stocker plusieurs identités et laisse Password Manager remplir automatiquement les formulaires en ligne, pour que vous puissiez par exemple faire des achats rapidement, facilement et en toute sécurité.

Comme tout le reste dans Password Manager, toutes les données sensibles associées à ces identités sont chiffrées et accessibles uniquement depuis l'appareil de l'utilisateur.





Pour ajouter une identité à Password Manager :

1. Sous Windows ou macOS, cliquez sur le  **Password Manager** icône dans votre navigateur Web.  
Sur Android ou iOS, lancez le  **Password Manager** application.  
Si vous y êtes invité, entrez votre [Mot de passe maître](#).
2. Ouvrez le menu Password Manager  pour développer la barre latérale gauche, puis cliquez sur  **Identités**.
3. Cliquez sur **Ajouter une identité** en bas de l'écran.
4. Saisissez les données requises puis cliquez sur **Enregistrer**.

### 5.3.2. Gestion des cartes bancaires

Cette fonctionnalité vous permet d'enregistrer les informations de vos cartes bancaires, pour que vous puissiez réaliser des transactions plus facilement, plus rapidement et en toute sécurité.

Pour ajouter une carte bancaire à Password Manager :

1. Sous Windows ou macOS, cliquez sur le  **Password Manager** icône dans votre navigateur Web.  
Sur Android ou iOS, lancez le  **Password Manager** application.  
Si vous y êtes invité, entrez votre [Mot de passe maître](#).
2. Ouvrez le menu Password Manager  pour développer la barre latérale gauche, puis cliquez sur  **Cartes bancaires**.
3. Appuyez sur le **Ajouter une identité** bouton en bas.







4. Complétez les détails que vous souhaitez enregistrer puis appuyez sur **Sauvegarder**.

### 5.3.3. Secure Me

La fonctionnalité Secure Me vous permet de vous déconnecter et d'effacer l'historique de navigation de votre ordinateur, tablette ou appareil mobile à distance. Nous vous recommandons vivement de l'activer si vous partagez un appareil avec d'autres personnes.





Pour trouver et activer cette fonctionnalité :

1. Sous Windows ou macOS, cliquez sur le  **Password Manager** icône dans votre navigateur Web.  
Sur Android ou iOS, lancez le  **Password Manager** application.  
Si vous y êtes invité, entrez votre [Mot de passe maître](#).
2. Ouvrez le menu Password Manager  pour développer la barre latérale gauche, puis cliquez sur  **Secure Me**.
3. Cliquez sur le bouton **Sécuriser toutes les sessions**.  
Si vous souhaitez sécuriser seulement un appareil, cherchez-le dans la liste des appareils sur lesquels Password Manager est installé ou activé sur un navigateur spécifique.

### 5.3.4. Notes

La fonctionnalité Notes sécurisées vous permet de disposer d'une sorte de carnet secret dans lequel vous pouvez stocker des données sensibles, les trier et les visualiser de manière optimale grâce à des codes couleur. Ainsi, vous pouvez non seulement organiser les informations comme vous le souhaitez, mais aussi les conserver en toute sécurité.

Pour localiser et activer cette fonctionnalité :

1. Sous Windows ou macOS, cliquez sur le  **Password Manager** icône dans votre navigateur Web.  
Sur Android ou iOS, lancez le  **Password Manager** application.  
Si vous y êtes invité, entrez votre [Mot de passe maître](#).
2. Ouvrez le menu Password Manager  pour développer la barre latérale gauche, puis cliquez sur  **Notes**.



3. Appuyez sur le bouton **Ajouter une note**.  
Écrivez les informations que vous souhaitez conserver puis cliquez sur **Enregistrer**.





## 6. FOIRE AUX QUESTIONS

Bitdefender Password Manager suscite quelques questions récurrentes. Nous avons les réponses ! Dans cette section, vous obtiendrez des informations supplémentaires sur votre compte Bitdefender, l'importation des mots de passe, les protocoles de sécurité des données et d'autres thématiques importantes pour nos clients.

### Questions générales sur Bitdefender Password Manager

#### **Comment supprimer le pop-up Password Manager qui apparaît dans ma solution de sécurité Bitdefender ?**

La notification Password Manager, qui s'affiche dans Bitdefender Total Security, Internet Security et Antivirus Plus depuis août 2022, peut être fermée en cliquant sur la croix qui se trouve en haut. La fenêtre « Gérez vos mots de passe avec Bitdefender Password Manager » réapparaîtra aléatoirement deux fois avant de disparaître définitivement. Vous pouvez empêcher l'affichage de ce message promotionnel en mettant le bouton {1}Notification des recommandations{2} en position Désactivée dans les paramètres de Bitdefender.

#### **Que se passe-t-il lorsque Bitdefender Password Manager expire ?**

Lorsque votre abonnement à Password Manager aura expiré et ne sera plus actif, vous disposerez de 90 jours pour exporter vos mots de passe. Ils seront sauvegardés pendant 30 jours de plus. Pendant ces 90 jours, vous pourrez seulement exporter vos données. Les fonctionnalités Remplissage automatique et Générateur de mots de passe seront désactivées.

À la fin de ces 90 jours, vous aurez 30 jours supplémentaires pour contacter Bitdefender et demander la restauration de vos mots de passe dans la base de données active, ce qui vous permettra de les exporter depuis Bitdefender Password Manager.

Vos données seront conservées dans la base de données active jusqu'à la fin du jour où vous aurez demandé leur restauration. À minuit, cette base de données sera effacée, et si vous n'avez pas dépassé la limite des 30 jours supplémentaires, vos mots de passe pourront à nouveau être restaurés depuis la sauvegarde. Les données de sauvegarde brutes



peuvent être fournies à l'utilisateur sur demande, mais la base de données est chiffrée et les informations ne sont pas accessibles.

### **Qu'est-ce que le mot de passe principal, et pourquoi dois-je m'en souvenir ?**

Le mot de passe principal est en quelque sorte la clé qui déverrouille l'accès à tous les mots de passe stockés dans votre compte Bitdefender Password Manager. Il doit comporter au moins 8 caractères. Choisissez un mot de passe fort, mémorisez-le et ne le donnez jamais à personne. Pour que votre mot de passe soit véritablement fort, nous vous recommandons de mélanger des majuscules, des minuscules, des chiffres et des caractères spéciaux (#, \$ ou @, par exemple).

### **Comment faire pour que Bitdefender ne me demande pas mon mot de passe principal à chaque fois que j'ouvre mon navigateur ?**

Si vous verrouillez votre appareil sans fermer votre navigateur, Password Manager ne se verrouille pas et vous pouvez accéder à vos données à votre retour. Par mesure de sécurité, à chaque ouverture de votre navigateur vous devez vous connecter à votre compte Bitdefender Central et saisir votre mot de passe principal.

- Pour empêcher l'affichage de la fenêtre de connexion à Bitdefender Central, rendez-vous dans  Paramètres et cochez la case Désactiver l'affichage de la fenêtre de connexion au démarrage.
- Pour éviter d'avoir à saisir votre mot de passe principal, cochez la case Se souvenir de moi dans la fenêtre Déverrouillage du coffre-fort.

### **Pourquoi mon mot de passe principal n'est-il pas conservé, et que faire si jamais je l'oublie ?**

Nous ne conservons pas votre mot de passe principal sur nos serveurs car c'est le moyen le plus sûr de faire en sorte que personne d'autre que vous ne puisse accéder à votre compte. Si Bitdefender Password Manager ne reconnaît pas votre mot de passe principal, vérifiez que vous n'avez pas fait d'erreur et que vous avez bien respecté la casse.

En cas d'oubli de votre mot de passe principal, vous pouvez toujours utiliser la clé de récupération pour déverrouiller Password Manager. Cette **clé de récupération** vous a été fournie pendant le processus d'installation de Bitdefender Password Manager et vous permet d'accéder de nouveau à votre compte sans perdre vos données.



Si vous avez oublié ou perdu le mot de passe principal et la clé de récupération, en dernier ressort, contactez un représentant Bitdefender qui vous aidera à réinitialiser votre compte.



### Important

Cette opération effacera toutes les données et tous les mots de passe enregistrés dans Bitdefender Password Manager.

### **Un abonnement à Bitdefender Password Manager peut-il être partagé par plusieurs utilisateurs ?**

Pour le moment ce n'est pas possible, mais nous y travaillons et nous proposerons prochainement cette option.

### **Qu'est-ce que le mode hors ligne et comment fonctionne-t-il ?**

Le mode hors ligne s'active automatiquement en cas de perte de la connexion Internet. Si vous aviez déjà saisi votre mot de passe principal Bitdefender Password Manager, il vous permet d'accéder à vos mots de passe même hors connexion.

### **Comment désinstaller Bitdefender Password Manager ?**

Pour désinstaller Bitdefender Password Manager :

- Sur Windows et macOS :  
Supprimez l'extension Password Manager de votre navigateur web. Faites un clic droit sur l'icône Bitdefender et sélectionnez Supprimer.
- Sous Android :  
Appuyez longuement sur l'icône de l'application Password Manager, puis faites-la glisser jusqu'en haut de l'écran, là où apparaît la mention Désactiver.
- Sur iOS et iPadOS :  
Appuyez longuement sur l'icône de l'application Password Manager jusqu'à ce que toutes les applications de l'écran bougent, puis appuyez sur la croix en haut à gauche de l'icône Bitdefender.

## Questions relatives à la vie privée et la sécurité

### **Les employés de Bitdefender peuvent-ils voir mes mots de passe ?**

Absolument pas. La protection de votre vie privée est notre priorité absolue. C'est d'ailleurs pour cela que nous ne conservons pas votre mot de passe principal dans nos serveurs de données : personne d'autre que



vous ne peut accéder à votre compte, pas même nos employés. Votre compte et tous les mots de passe associés sont chiffrés à l'aide des algorithmes de sécurité les plus puissants à ce jour, et le code que nous voyons n'est qu'une combinaison de chiffres et de lettres.

### **Que se passerait-il en cas de piratage des serveurs de Password Manager ?**

Chaque mot de passe est chiffré localement sur votre appareil avant d'arriver sur nos serveurs. Si des pirates décidaient de s'en prendre à notre système, ils n'y trouveraient que des pages entières de chiffres et de lettres car il leur manquerait votre clé pour les déchiffrer. Cela signifie que vous et vos données êtes en parfaite sécurité avec nous.



## 7. OBTENIR DE L'AIDE

### 7.1. Demander de l'aide

Bitdefender offre à ses clients une assistance sans égale, rapide et précise. Si vous rencontrez des difficultés ou si vous avez la moindre question au sujet de votre produit Bitdefender, nous mettons à votre disposition plusieurs ressources en ligne dans lesquelles vous trouverez sûrement une solution ou une réponse. Vous pouvez également contacter le service client Bitdefender. Nos représentants vous répondront dans les plus brefs délais et vous fourniront toute l'aide dont vous avez besoin.

### 7.2. Ressources En Ligne

De nombreuses ressources en ligne sont disponibles pour vous aider à trouver des réponses à vos questions et résoudre les problèmes liés à Bitdefender.

- Centre de Support Bitdefender :  
<https://www.bitdefender.fr/consumer/support/>
- Communauté des experts Bitdefender :  
<https://community.bitdefender.com/fr>
- Bitdefender Cyberpedia:  
<https://www.bitdefender.com/cyberpedia/>

Vous pouvez également utiliser le moteur de recherche de votre choix pour obtenir plus d'informations sur la sécurité informatique, les produits et l'entreprise Bitdefender.

#### 7.2.1. Centre de support Bitdefender

Le Centre de Support de Bitdefender est une base en ligne d'informations concernant les produits Bitdefender. Il contient, dans un format facilement accessible, les rapports d'incidents survenus, ainsi que les bugs constatés, par le support technique de Bitdefender. Vous y découvrirez également des articles généraux sur la prévention contre les menaces, sur la gestion, en détail, des solutions Bitdefender et beaucoup d'autres articles.

La base de connaissances de Bitdefender est ouverte au public et consultable gratuitement. Cet ensemble d'information est une autre



manière de fournir aux clients de Bitdefender les informations techniques dont ils ont besoin. Toutes les requêtes valides d'information ou les rapports de bug venant de clients de Bitdefender trouvent une réponse en cherchant dans la base de données de Bitdefender, comme les rapports de bugs, travaux associés, feuillet ou article d'information venant compléter les fichiers d'aide des produits.

Le centre de support Bitdefender est accessible à tout moment à l'adresse suivante : <https://www.bitdefender.fr/consumer/support/>.

### 7.2.2. Communauté des experts Bitdefender

La communauté des experts est un espace dans lequel des utilisateurs et des amateurs des produits Bitdefender peuvent échanger, s'entraider et partager leurs connaissances et leurs solutions. C'est aussi un espace propice à l'émergence d'idées et de commentaires précieux pour nos développeurs. Les membres de la communauté sont des utilisateurs expérimentés heureux de donner un peu de leur temps pour aider les autres. Grâce à leurs généreux efforts, nous avons créé une base de connaissances dans laquelle tous les utilisateurs peuvent une aide et un peu de convivialité.

Vous pourrez avoir des conversations riches avec des personnes qui utilisent vraiment les produits Bitdefender. Cette communauté permet aux membres d'établir des liens et de faire entendre leurs voix. Ils sont encouragés à y participer en sachant que leurs opinions et leurs contributions sont respectées et appréciées. En tant que fournisseur reconnu, nous nous efforçons d'offrir à nos clients une assistance rapide et précise et nous voulons nous rapprocher d'eux. C'est dans cette optique nous avons créé cette communauté.

Vous pouvez rejoindre la communauté des experts ici :

<https://community.bitdefender.com/fr>

### 7.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia regroupe toutes les dernières informations sur les cybermenaces. c'est là que les experts Bitdefender partagent des conseils et des astuces sur la protection contre les pirates, les violations de données et l'usurpation d'identité, notamment sur les réseaux sociaux.

La page Bitdefender Cyberpedia se trouve ici :

<https://www.bitdefender.com/cyberpedia>.



## 7.3. Pour nous joindre

Une communication efficace est la clé d'une relation professionnelle réussie. Depuis 2001, BITDEFENDER s'est bâti une réputation irréprochable en cherchant sans cesse à améliorer sa communication pour dépasser les attentes de ses clients et de ses partenaires. Si vous avez la moindre question, n'hésitez pas à nous contacter directement via **Bitdefender Support Center**.

<https://www.bitdefender.fr/consumer/support/>

### 7.3.1. Distributeurs locaux

Les distributeurs locaux Bitdefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de sujets commerciaux ou généraux.

Pour trouver un distributeur Bitdefender dans votre pays :

1. Rendez-vous sur <https://www.bitdefender.com/partners/partner-locator.html>.
2. Choisissez vos pays et ville à l'aide des options correspondantes.



## GLOSSAIRE

### **Code d'activation**

Clé unique qui peut être achetée chez un revendeur et utilisée pour activer un produit ou service spécifique. Un code d'activation permet l'activation de l'abonnement valide pour un certain laps de temps et pour certains appareils, et peut également être utilisé pour prolonger un abonnement avec pour seule condition d'être utilisé pour le même produit ou service.

### **ActiveX**

ActiveX est un modèle pour écrire des programmes afin que d'autres programmes et le système d'exploitation puissent les appeler. La technologie ActiveX est utilisée par Microsoft Internet Explorer pour créer des pages Web interactives qui ressemblent et se comportent comme des programmes informatiques classiques, plutôt que comme des pages statiques. Avec ActiveX, les utilisateurs peuvent poser ou répondre à des questions, utiliser des boutons et interagir de multiples façons avec les pages Web. Les commandes ActiveX sont souvent écrites en Visual Basic. ActiveX est connu pour son manque total de contrôles de sécurité ; les experts en sécurité informatique déconseillent son utilisation sur Internet.

### **Menaces persistantes avancées**

Les Menaces persistantes avancées exploitent les vulnérabilités des systèmes pour voler des informations importantes et les livrer à la source. Les grands groupes tels que les entreprises, les sociétés ou les gouvernements sont ciblés par cette menace. L'objectif d'une menace persistante avancée est de passer inaperçue pendant le plus de temps possible, tout en surveillant et regroupant des informations importantes sans endommager les machines ciblées. La méthode utilisée pour injecter la menace dans le réseau consiste à faire ouvrir un fichier PDF ou un document Office qui a l'air inoffensif, pour que chaque utilisateur puisse exécuter les fichiers.

### **Adware**

Les publiciels sont souvent associés à des applications gratuites qui exigent leur acceptation par l'utilisateur. Ces publiciels étant généralement installés une fois que l'utilisateur en a accepté le





principe dans un accord de licence, ils ne peuvent pas être considérés comme illégaux. Cependant, les fenêtres publicitaires peuvent devenir contrariantes et, dans certains cas, nuire aux performances du système. De plus, les informations recueillies peuvent mettre en péril la vie privée des utilisateurs qui n'ont pas totalement pris connaissance des conditions de l'accord de licence.

### **Archive**

Une disquette, une bande, ou un répertoire qui contient des fichiers qui ont été sauvegardés.

Un fichier qui contient un ou plusieurs fichiers dans un format compressé.

### **Porte dérobée**

Il s'agit d'une faille dans la sécurité d'un système délibérément laissé en place par des développeurs ou mainteneurs. La motivation n'est pas toujours négative ; quelques logiciels permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.

### **Secteur de démarrage**

Un secteur au début de chaque disque qui identifie l'architecture du disque (taille des secteurs, etc). Pour les disques de démarrage, le secteur de boot contient aussi un programme qui charge la plate-forme.

### **Virus de démarrage**

Menace qui infecte le secteur d'amorçage d'une disquette ou d'un disque dur. Une tentative de démarrer depuis une disquette infectée avec un virus d'amorçage rendra la menace active en mémoire. Chaque fois que vous démarrez votre système depuis ce point, vous aurez la menace active en mémoire.

### **Botnet**

Le terme « botnet » est un mot composé de robot et de network (réseau). Les botnets sont des appareils connectés à Internet infectés par une menace et pouvant servir à envoyer des pourriels, voler des données, contrôler à distance les appareils vulnérables ou diffuser des logiciels espions, rançongiciels, ou tout autre type de menace. Leur objectif est d'infecter autant d'appareils connectés que possible, comme les PC, serveurs, mobiles ou autres objets connectés appartenant à des grandes entreprises.



### **Navigateur**

Raccourci pour navigateur internet, il s'agit d'un logiciel utilisé pour visualiser des pages Web. Les principaux navigateurs comprennent Microsoft Internet Explorer, Mozilla Firefox et Google Chrome. Ce sont des navigateurs graphiques, ce qui signifie qu'ils peuvent afficher aussi bien le graphisme que le texte. De plus, les navigateurs les plus modernes peuvent visionner les informations multimédia, y compris le son et la vidéo, bien qu'ils exigent des modules d'extension (plugiciels) pour certains formats.

### **Attaque par force brute**

Les attaques qui essaient de pénétrer un système informatique en saisissant toutes les combinaisons de mots de passe possible, ce en commençant par les mots de passe les plus faciles à deviner.

### **Ligne de commande**

Dans une interface en ligne de commande, l'utilisateur tape directement des commandes correspondant à des ordres de gestions.

### **Cookies**

Sur Internet, les témoins sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des témoins est encore en développement. Son but est de cibler directement les intérêts que vous avez exprimés. C'est une arme à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent car vous voyez seulement les annonces vous intéressant. Mais cela implique également le "pistage" et le "suivi" des sites que vous consultez et de ce sur quoi vous cliquez. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple "code SKU" (ce code barres se trouvant au dos des produits de consommation). Bien que ce point de vue puisse paraître extrême, il est parfois justifié.

### **Cyberharcèlement**

Lorsque des camarades ou des inconnus mènent des actions abusives envers des enfants dans le but de les blesser physiquement. Pour leur nuire sur le plan émotionnel, les assaillants envoient des messages malveillants ou des photos peu flatteuses, provoquant l'isolation de leurs victimes ou un sentiment de frustration.



### **Attaque par dictionnaire**

Les attaques qui essaient de pénétrer un système informatique en saisissant une combinaison de mots communs pour générer des mots de passe potentiels. La même méthode est utilisée pour deviner les clés de chiffrements des messages ou documents chiffrés. Les attaques par dictionnaire fonctionnent car de nombreuses personnes ont tendance à choisir des mots de passe simples à deviner et ne contenant qu'un seul mot.

### **Lecteur de disque**

C'est un appareil qui lit et écrit des données sur un disque. Une unité de disque dur lit et écrit sur un disque dur. Un lecteur de disquette accède à des disquettes. Les lecteurs peuvent être soit internes (intégrés à un ordinateur) soit externes (intégrés dans un boîtier séparé que l'on connecte à l'ordinateur).

### **Télécharger**

Copier des données (généralement un fichier entier) d'une source principale à un dispositif périphérique. Le terme est souvent utilisé pour décrire le processus de copie d'un fichier d'un service en ligne vers son ordinateur. Le téléchargement peut aussi se référer à la reproduction d'un fichier d'un serveur de réseau vers un ordinateur sur le réseau.

### **E-mail**

Courrier électronique. Il s'agit d'un service d'envoi de messages sur des ordinateurs via un réseau local ou global.

### **Événements**

Il s'agit d'une action ou d'une occurrence détectée par un programme. Les événements peuvent être des actions d'utilisateur, comme le clic sur un bouton de souris ou la pression d'une touche, ou des occurrences du système, comme l'analyse de la mémoire.

### **Exploits**

Une manière de tirer profit des bugs et vulnérabilités (logicielles ou matérielles) qui sont présents sur un ordinateur. Les pirates peuvent ainsi prendre le contrôle des ordinateurs ou réseaux.

### **Faux positif**

Se produit lorsqu'une analyse identifie un fichier comme infecté alors qu'il ne l'est pas.



### **Extension du nom de fichier**

La partie d'un fichier, après le point final, qui indique le type de données stockées dans le fichier. De nombreux systèmes d'exploitation utilisent des extensions de fichiers, par exemple Unix, VMS, MS-DOS. Elles comportent communément une à trois lettres (certains systèmes plus anciens n'en supportent pas plus de trois). Exemples: "c" pour du code source en C, "ps" pour PostScript, "txt" pour du texte.

### **Heuristique**

Méthode basée sur des règles permettant d'identifier de nouvelles menaces. Cette méthode d'analyse ne s'appuie pas sur une base de données d'information sur les menaces spécifique. L'avantage de l'analyse heuristique est de pouvoir détecter les variantes d'une menace existante. Cependant, cette méthode peut parfois occasionner de fausses alertes dans des programmes normaux.

### **Pot de miel**

Un faux système informatique est créé pour attirer les pirates informatiques afin d'étudier la façon dont ils agissent et identifient les méthodes hérétiques utilisées pour collecter des informations sur le système. Les sociétés et les entreprises sont plus intéressées par la mise en place et l'utilisation de pots de miel pour améliorer leur état de sécurité global.

### **IP**

Protocole Internet - Un protocole routable de la suite de protocoles TCP/IP chargé de l'adressage, du routage IP et de la fragmentation et réassemblage des paquets IP.

### **Applet Java**

Il s'agit d'un programme Java conçu pour s'exécuter uniquement dans une page Web. Pour utiliser un applet dans une page Web, vous devez spécifier le nom de l'applet et la taille (la longueur et la largeur - en pixels) qu'il peut utiliser. Lors d'un accès à la page Web, le navigateur télécharge l'applet depuis un serveur et l'exécute sur la machine de l'utilisateur (le client). Les applets diffèrent des applications par le fait qu'ils sont régis par un protocole de sécurité strict.

Par exemple, bien que les applets s'exécutent sur le client, ils ne peuvent pas lire ou écrire des données sur la machine du client. De plus, les



applets sont également limités pour ne pouvoir lire et écrire des données que depuis le domaine les hébergeant.

### **Enregistreur de frappe**

Un enregistreur de frappe est une application qui enregistre tout ce qui est saisi avec le clavier. Les enregistreurs de frappe ne sont pas nécessairement malveillants. Ils peuvent être utilisés à des fins légitimes, comme pour surveiller les activités d'employés ou d'enfants. Ils sont toutefois de plus en plus utilisés par les cybercriminels à des fins malveillantes (par exemple, pour recueillir des informations confidentielles, telles que des identifiants de connexion ou des numéros d'assurance sociale).

### **Virus macro**

Type de menace codée sous la forme d'une macro intégrée dans un document. Beaucoup d'applications, telles Microsoft Word et Excel, supportent de puissants langages macro. Ces applications vous permettent d'intégrer une macro dans un document, et de le faire s'exécuter chaque fois que le document est ouvert.

### **Client de messagerie**

Un client de messagerie est une application qui vous permet d'envoyer et recevoir des e-mails.

### **Mémoire**

Zone de stockage interne dans votre ordinateur. Le terme mémoire regarde le stockage des données dans les "chips" (composants), et le terme stockage regarde les disques. Chaque ordinateur a une certaine quantité de mémoire physique, appelée mémoire vive ou RAM.

### **Non-heuristique**

Cette méthode d'analyse s'appuie sur une base de données d'information sur les menaces spécifique. L'avantage de l'analyse non-heuristique est qu'elle n'est pas trompée par ce qui peut sembler être une menace et ne génère donc pas de fausses alertes.

### **Prédateurs en ligne**

Individus cherchant à discuter avec des mineurs et des adolescents dans le but de les impliquer dans des activités sexuelles illégales. Les réseaux sociaux sont l'endroit idéal pour traquer les enfants vulnérables et les séduire dans le but de les faire se livrer à des activités sexuelles, en ligne ou en face à face.



### **Programmes compressés**

Fichier dans un format compressé. Beaucoup de systèmes d'exploitation et d'applications contiennent des commandes vous permettant de compresser un fichier afin qu'il occupe moins de mémoire. Par exemple, imaginons que vous avez un fichier texte contenant dix caractères "espace vide" à la suite. Normalement, cela nécessite 10 octets.

Pourtant, un logiciel qui comprime les fichiers remplace la série d'espaces par un caractère spécial série d'espaces suivi du nombre d'espaces remplacés. Dans ce cas, les dix espaces nécessitent seulement 2 octets. C'est juste une technique de compression, il y en a une multitude.

### **Chemin**

Les directions exactes vers un fichier. Ces directions sont décrites d'habitude par arborescence, de haut en bas.

La connexion entre deux points, comme le canal de communication entre deux ordinateurs.

### **Phishing**

Action d'envoyer un courriel à un utilisateur en prétendant être une entreprise connue dans le but d'obtenir frauduleusement des informations privées qui permettront d'utiliser l'identité du destinataire du courriel. Cet courriel oriente l'utilisateur vers un site Web où il lui est demandé de mettre à jour des informations personnelles, comme ses mots de passe, son numéro de carte de crédit, de sécurité sociale ou de compte en banque, que les véritables entreprises connaissent déjà. Ce site Web est bien sûr totalement factice et n'a pour objectif que de voler les informations de l'utilisateur.

### **Photon**

Photon est une technologie Bitdefender innovante et discrète, conçue pour limiter l'impact de la solution de sécurité sur les performances. En surveillant l'activité de votre PC en tâche de fond, elle crée des modèles d'utilisation qui aident à optimiser les processus de démarrage et d'analyse.

### **Virus polymorphe**

Menace qui change de forme avec chaque fichier qu'elle infecte. Ces menaces n'ayant pas de forme unique bien définie, elles sont plus difficiles à identifier.



### **Port**

Une interface de l'ordinateur à laquelle vous pouvez connecter un périphérique. Les PCs comportent plusieurs sortes de ports. A l'intérieur, il y a quelques ports pour la connexion des disques, cartes vidéo. A l'extérieur, les PCs ont des ports pour connecter des modems, imprimantes, souris et autres périphériques.

Dans des réseaux TCP/IP et UDP, un point final pour une connexion logique. Le numéro du port identifie son type. Par exemple, le port 80 est utilisé pour le trafic HTTP.

### **Ransomware**

Les ransomwares sont des programmes malveillants qui tentent de soutirer de l'argent aux utilisateurs en bloquant leurs systèmes vulnérables. CryptoLocker, CryptoWall, et TeslaWall ne sont que des variantes qui traquent les systèmes personnels des utilisateurs.

L'infection peut se répandre via courriel, le téléchargement de pièces jointes, ou l'installation d'applications, sans prévenir l'utilisateur de ce qui se passe dans son système. Les utilisateurs quotidiens et les entreprises sont ciblés par les pirates derrière les rançongiciels.

### **Fichier de rapport**

Un fichier qui enregistre les actions qui surviennent. BitDefender maintient un fichier journal contenant les chemins analysés, les dossiers, le nombre d'archives et de fichiers analysés, le nombre de fichiers suspects et infectés.

### **Rootkit**

Un rootkit est un ensemble d'outils logiciels permettant aux administrateurs d'accéder à un système. Le terme a été utilisé initialement pour les systèmes d'exploitation UNIX se réfère à des outils recompilés fournissant des droits administrateurs "intrusifs", permettant de cacher leur présence aux administrateurs systèmes.

Le principal rôle des rootkits est de cacher des processus, des fichiers, des logins et des logs. Ils peuvent également intercepter des données depuis des terminaux, des connexions réseau, s'ils incluent les logiciels appropriés.

Les trousseaux administrateur ne sont pas nécessairement malveillants. Par exemple, les systèmes d'exploitation et même certaines applications



cachent des fichiers sensibles en utilisant des trousseaux administrateur. Cependant, ils sont principalement utilisés pour camoufler des menaces ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des menaces, les trousseaux administrateur pirates sont une menace importante contre l'intégrité et la sécurité d'un système. Ils peuvent analyser le trafic, créer des portes dérobées sur le système, modifier des fichiers et des journaux et passer inaperçus.

### **Script**

Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention utilisateur.

### **Spam**

Message électronique ou envoi de messages souvent répertoriés comme des e-mails « non sollicités ».

### **Spyware**

Tout type de logiciel récupérant les informations des utilisateurs via leur connexion Internet à leur insu, généralement à des fins publicitaires. Les logiciels espions sont généralement cachés dans des logiciels gratuits et logiciels gratuits pouvant être téléchargés sur Internet. Notons toutefois que la plupart des logiciels gratuits ne contiennent pas de logiciels espions. Une fois installé, le logiciel espion surveille l'activité de l'utilisateur sur internet et transmet discrètement ces informations à une tierce personne. Les spywares peuvent également récupérer des informations sur les adresses mail, les mots de passe ou même, les numéros de cartes bancaires.

Leur point commun avec les chevaux de Troie est le fait que les utilisateurs les installent involontairement en même temps qu'un autre produit. Une des manières les plus classiques d'être victime de logiciels espions est de télécharger des logiciels de partage de fichiers (Peer to peer).

En plus des questions d'éthique et de respect de la vie privée, les logiciels espions volent les ressources de l'ordinateur de l'utilisateur en utilisant sa bande passante lors de l'envoi d'informations à leur base via la connexion Internet. En raison de cette utilisation de la mémoire et des ressources du système, les applications qui fonctionnent en tâche de fond peuvent aller jusqu'à entraîner des plantages ou provoquer une instabilité globale du système.

### **Éléments de démarrage**





Tous les fichiers placés dans ce dossier s'ouvrent au démarrage de l'ordinateur. Par exemple, un écran de démarrage, un fichier son pour le démarrage de l'ordinateur, un calendrier, des programmes, peuvent être placés dans ce dossier. C'est généralement un raccourci vers le fichier qui est placé dans le dossier, et pas le fichier.

### **Abonnement**

Achetez une licence qui donne à l'utilisateur le droit d'utiliser un produit ou service particulier sur un nombre spécifique d'appareils et pour un certain laps de temps. Un abonnement expiré peut être renouvelé automatiquement en utilisant les informations données par l'utilisateur lors du premier achat.

### **Barre d'état**

Introduite avec Windows 95, la zone de notification se situe dans la barre de tâches Windows (en général, à côté de l'horloge) et contient des icônes miniatures permettant d'accéder facilement aux fonctions système : fax, imprimante, modem, volume, etc. Double-cliquez ou faites un clic-droit sur une icône pour afficher les options.

### **TCP/IP**

Transmission Control Protocol/Internet Protocol - Ensemble de protocoles réseau utilisés largement sur internet assurant la communication entre des réseaux interconnectés d'ordinateurs avec diverses architectures matérielles et divers systèmes d'exploitation. TCP/IP inclut des normes pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.

### **Menace**

Programme ou morceau de code chargé dans votre ordinateur à votre insu et qui fonctionne contre votre gré. La plupart des menaces peuvent également se répliquer. Toutes les menaces informatiques sont créées par des personnes. Une menace simple peut se copier très rapidement et sans arrêt et est relativement facile à créer. Même une menace simple comme celle décrite est dangereuse puisqu'elle remplit vite la mémoire et bloque le système. Une menace plus dangereuse encore est par exemple capable de se transmettre via un réseau et de déjouer les systèmes de sécurité.



### **Mise à jour des informations sur les menaces**

La signature binaire de la menace, utilisée par la solution de sécurité pour détecter et éliminer la menace.

### **Cheval de Troie**

Programme destructeur qui prétend être une application normale. À la différence des programmes malveillants comme les vers, les chevaux de Troie ne se répliquent pas, mais ils peuvent être tout autant destructeurs. L'un des types les plus pernicioeux de chevaux de Troie est un programme qui, sous couvert de supprimer les menaces de votre ordinateur, en installe en fait de nouvelles.

Le terme provient de la fameuse histoire de l'Iliade écrite par Homère, dans laquelle les Grecs font un cadeau de "paix" à leurs ennemis, les Trojans, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur ville qu'ils se rendent compte que le cheval est plein de soldats grecs, qui ouvrent les portes de la ville, permettant aux attaquants de capturer Troie.

### **Mise à jour**

Une nouvelle version du logiciel ou d'un produit hardware, destinée à remplacer une ancienne version du même produit. D'habitude, les installations de mises à jour vérifient si le produit initial est installé, sinon la mise à jour ne se fait pas.

BitDefender a son propre module de mise à jour permettant à l'utilisateur de vérifier manuellement les mises à jour ou de les programmer automatiquement.

### **VPN (réseau virtuel privé)**

C'est une technologie qui permet une connexion temporaire et chiffrée à un certain réseau plutôt qu'à un autre moins sécurisé. De cette façon, l'envoi et la réception de données sont protégés et chiffrés et plus difficiles à intercepter pour les pirates. Une preuve de sécurité est l'identification, qui ne peut se faire que via un identifiant et un mot de passe.

### **Ver**

Un programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure qu'il se propage. Il ne peut pas s'attacher aux autres programmes.