

Bitdefender[®]

PASSWORD MANAGER



**GUIDE
D'UTILISATION**



Bitdefender Password Manager

Guide de l'utilisateur

Date de publication : 21/11/2022
Copyright © 2022 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

À propos de ce guide	1
Objectifs et destinataires	1
Comment utiliser ce guide	1
Conventions utilisées dans ce guide	1
Normes typographiques	1
Avertissement	2
Commentaires	2
1. Qu'est-ce que Bitdefender Password Manager	4
1.1. La sécurité et son fonctionnement	4
1.2. Versions d'essai et payantes de Password Manager	4
1.3. Gestionnaire de portefeuille et de mots de passe Bitdefender	5
2. Commencer	7
2.1. Configuration requise	7
2.1.1. Logiciels	8
2.2. Installation	8
2.2.1. Installation sur les appareils Windows et macOS	8
2.2.2. Installation sur les appareils Android	10
2.2.3. Installation sur les appareils iOS	12
3. Importation et exportation de vos mots de passe	15
3.1. Compatibilité	15
3.2. Importation des données dans Password Manager	16
3.3. Exportation des données depuis Password Manager	18
3.4. Transfert de votre Bitdefender Wallet vers Password Manager	20
4. Caractéristiques et fonctionnalités	22
4.1. Gestion des mots de passe	22
4.1.1. Générateur de mots de passe	22
4.1.2. Capture des mots de passe	23
4.1.3. Remplissage automatique intelligent	23
4.1.4. Rapport de sécurité	23
4.1.5. Synchronisation sur de multiples plateformes	24
4.1.6. Suppression des mots de passe	24
4.2. Gestion des comptes	24
4.2.1. Authentification	24
4.2.2. Réinitialisation du mot de passe principal	25
4.3. Autres fonctionnalités	27
4.3.1. Gestion des identités	27
4.3.2. Gestion des cartes bancaires	27
4.3.3. Secure Me	28
4.3.4. Notes	28



- 5. Questions fréquemment posées 30
- 6. Obtenir de l'aide 34
 - 6.1. Demander de l'aide 34
 - 6.2. Ressources en ligne 34
 - 6.2.1. Centre de support Bitdefender 34
 - 6.2.2. Communauté des experts Bitdefender 35
 - 6.2.3. Bitdefender Cyberpedia 35
 - 6.3. Pour nous joindre 37
 - 6.3.1. Distributeurs locaux 37
- Glossaire 38



À PROPOS DE CE GUIDE

Objectifs et destinataires

Ce guide est destiné à tous les utilisateurs de Bitdefender sur tous les systèmes d'exploitation pris en charge (Windows, MacOS, Android, iOS) qui ont choisi Bitdefender Password Manager comme outil de gestion de mot de passe incontournable. Les informations présentées dans ce livre conviennent non seulement aux alphabétisés en informatique, mais elles servent de guide accessible et convivial pour tous.

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 :

[Commencer \(page 7\)](#)

Installation et démarrage de {1}{2}

[Caractéristiques et fonctionnalités \(page 22\)](#)

Utilisation de {1}{2} et de toutes ses fonctionnalités

[Obtenir de l'aide \(page 34\)](#)

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 échantillons de syntaxe sont imprimés avec <code>monospaced</code> personnages.
https://www.bitdefender.com	Les liens URL renvoient vers un emplacement externe comme un serveur http ou ftp.
documentation@bitdefender.com	Les adresses email sont insérées dans le texte pour plus d'informations sur les contacts.
À propos de ce guide (page 1)	Ceci représente un lien interne vers un emplacement à l'intérieur de ce document.
filename	Les fichiers et les répertoires sont imprimés à l'aide de <code>monospaced</code> personnages.
option	Toutes les options du produit sont imprimées à l'aide gras personnages.
mot-clé	Les mots-clés ou expressions importants sont mis en évidence à l'aide de gras personnages.

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.



Avertissement

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.

Faites-le nous savoir en envoyant un courriel à documentation@bitdefender.com. Rédigez tous vos e-mails liés à la documentation en anglais afin que nous puissions les traiter efficacement.



1. QU'EST-CE QUE BITDEFENDER PASSWORD MANAGER

Bitdefender Password Manager est un service multiplateforme conçu pour aider les utilisateurs à stocker et à organiser tous leurs mots de passe en ligne. Il est construit avec les algorithmes cryptographiques les plus puissants connus pour le plus haut niveau de sécurité et de sécurité numérique. Il fonctionne comme une extension de navigateur et une solution d'application mobile pour la gestion des identités et des mots de passe, les opérations bancaires et tous les autres types d'informations sensibles sur tous les appareils.

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

1.1. La sécurité et son fonctionnement

Derrière la Bitdefender Password Manager Le logiciel contient certains des derniers algorithmes cryptographiques qui garantissent la plus haute sécurité des données que les utilisateurs peuvent espérer, tels que les protocoles AES-256-CCM, SH512, BCRYPT, HTTPS et WSS pour la transmission de données. Toutes les données concernées sont à tout moment cryptées et décryptées localement. Cela fait en sorte que seul le titulaire du compte peut avoir accès aux informations stockées dans le compte, ainsi qu'au mot de passe principal qui est utilisé pour accéder et ensuite utiliser les données en question.

1.2. Versions d'essai et payantes de Password Manager

La version d'essai de Bitdefender Password Manager fonctionne avec tous les comptes identiques à la version payante du produit, mais sa disponibilité expirera après 90 jours après son activation.



Note

Notez que la version payante du produit, bien qu'elle puisse être achetée en tant que produit purement autonome, un accès illimité à Password Manager est inclus dans les abonnements Bitdefender Premium Security et Bitdefender Ultimate Security.

1.3. Gestionnaire de portefeuille et de mots de passe Bitdefender

De nombreux utilisateurs qui ont déjà rencontré ou utilisé notre fonctionnalité Bitdefender Wallet dans le passé ont été attirés par le "Gestionnaire de mots de passe" en apparence d'une version améliorée des systèmes déjà existants que nous avons en place. Nous pensons qu'il est très important de bien faire la distinction entre ces produits.

Bitdefender Wallet et Bitdefender Password Manager ne sont pas le même produit, la principale différence étant la synchronisation multiplateforme des mots de passe. Password Manager est un logiciel autonome compatible avec les appareils Windows, Android, macOS et iOS, tandis que Wallet est un module de gestion de mots de passe avec des fonctionnalités de base fourni avec nos solutions de sécurité payantes (Bitdefender Antivirus Plus, Bitdefender Internet Security, Bitdefender Total Security). Le portefeuille est disponible uniquement sur Windows, étant incompatible avec tous les autres systèmes d'exploitation.

- Wallet s'intègre uniquement avec les navigateurs suivants : Chrome, Firefox, Internet Explorer et Bitdefender Safepay.
- Contrairement au gestionnaire de mots de passe, le portefeuille ne fournit à l'utilisateur aucune option de récupération du mot de passe principal. Cela signifie que la perte de votre mot de passe maître implique la perte de tous les mots de passe gérés par le module Wallet.
- Les fonctions de portefeuille sont limitées à la sauvegarde automatique et au remplissage automatique, au verrouillage automatique et au générateur de mot de passe.
- Vous pouvez importer des données dans votre portefeuille à partir d'autres applications de gestion de mot de passe uniquement dans **.db** et **.csv** formats.



Nous explorerons plus en détail et discuterons en détail des fonctionnalités disponibles pour Password Manager et de toutes les améliorations et fonctionnalités supplémentaires qui le différencient de notre module Wallet intégré.



2. COMMENCER

2.1. Configuration requise

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

- **Pour les utilisateurs de PC:**

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

- **Pour les utilisateurs de 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 iOS:**

- Système d'exploitation iOS 11.0 ou ultérieur

- **Pour les utilisateurs d'Android:**

- Système d'exploitation Android 5.1 ou ultérieur



Note

- La fonction de déverrouillage par empreinte digitale est prise en charge sur **Android 6.0** et ensuite.
- La fonction de remplissage automatique est prise en charge sur **Android 8.0** et plus tard, compatible avec iPhone, iPad et iPod touch.



2.1.1. Logiciels

Pour pouvoir utiliser Bitdefender Password Manager et toutes ses fonctionnalités, vos appareils Windows ou macOS doivent répondre aux exigences logicielles suivantes:

- **Bord Microsoft** (basé sur Chromium 80 et versions ultérieures)
- **MozillaFirefox** (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

Le non-respect des exigences système présentées ci-dessus entraînera soit l'impossibilité d'installer Bitdefender Password Manager ou le dysfonctionnement du produit.

2.2. Installation

Ce chapitre vous guidera sur la façon d'installer Bitdefender Password Manager à la fois sur les navigateurs Web de votre PC Windows et macOS, ainsi que sur vos appareils mobiles Android ou iOS.



Important

Avant l'installation, assurez-vous que vous disposez d'un abonnement valide à Password Manager dans votre [Centrale Bitdefender](#) compte afin que cette extension de navigateur puisse récupérer sa validité à partir de votre compte.

Les abonnements actifs sont répertoriés dans le **Mes abonnements** section dans 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.



Les navigateurs actuellement pris en charge pour le produit sont les suivants : **Google Chrome, MozillaFirefox, Bord Microsoft, et Safari.**

1. Aller à <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. 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. 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 le **Obtenir** bouton
- ☐ Cliquez sur **Ajouter une extension** dans l'invite qui s'affiche à l'écran

Google Chrome

- ☐ Cliquez le **Ajouter à Chrome** bouton
- ☐ Dans la boîte de confirmation, cliquez sur **Ajouter une extension**

Mozilla Firefox

- ☐ Cliquez le **Ajouter à Firefox** bouton
- ☐ Cliquez le **Installer** bouton dans le coin supérieur droit de l'écran

Safari



- Cliquez le **Obtenir** bouton, puis cliquez sur **Installer**
- Ouvrez Safari et sélectionnez **Préférences** dans la barre de menu supérieure
- Dans la fenêtre Préférences, cliquez sur le **Rallonges** languette
- Cochez la case à côté de Password Manager pour l'activer

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

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

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 **oublier le mot de passe maître** précédemment configuré pour votre compte.

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

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 de l'application Bitdefender Password Manager peut également être effectuée via votre **Centrale Bitdefender** compte:

1. Sur votre appareil mobile Android, connectez-vous à votre compte Bitdefender Central en accédant à <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. Vous serez redirigé vers [jeu de Google](#). Cliquez sur **Installer** pour télécharger Bitdefender Password Manager sur Android.
7. Une fois le téléchargement terminé, ouvrez le  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. 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.
10. Appuyez sur **Activer le remplissage automatique** pour configurer les paramètres de remplissage automatique d'Android.



Note

Si vous ignorez cette étape, vous pouvez activer et personnaliser les fonctionnalités de remplissage automatique d'Android ultérieurement en suivant les instructions disponibles sur [Remplissage automatique intelligent \(page 23\)](#).

11. Une liste d'applications de remplissage automatique des mots de passe s'affiche.
Sélectionner **Gestionnaire de mots de passe** puis l'appareil vous demandera de confirmer que vous faites confiance à cette application.
Robinet **D'ACCORD**.
12. Entrez le code PIN que vous avez configuré dans **étape 9** pour confirmer cette action.

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 iPad, connectez-vous à votre compte Bitdefender Central en accédant <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. Vous serez redirigé vers **Magasin d'applications**. Appuyez sur l'icône du nuage avec une flèche pointant vers le bas pour télécharger Bitdefender Password Manager pour iOS.
7. Une fois la  est installée, ouvrez-la et cochez la petite case à l'écran. Sélectionner **Continuer** après avoir lu et accepté les **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. IMPORTATION ET EXPORTATION DE VOS MOTS DE PASSE

Bitdefender Password Manager est conçu de manière à faciliter efficacement la communication et le transfert de données avec des sources, plates-formes et outils logiciels externes. C'est la raison principale pour laquelle le besoin très fréquemment rencontré d'importer ou d'exporter des mots de passe vers ou depuis Bitdefender Password Manager peut être facilement satisfait.

3.1. Compatibilité

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

- ☐ 1Password
- ☐ Bitwarden
- ☐ Bitdefender Password Manager
- ☐ Bitdefender Wallet
- ☐ 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 de l'outil de gestion de mots de passe à partir duquel vous essayez de transférer des fichiers de données n'est pas mentionné dans la liste fournie ci-dessus, vous pouvez suivre notre guide en ligne sur la façon dont les utilisateurs peuvent modifier un fichier CSV à partir de gestionnaires de mots de passe non pris en charge afin que vous puissiez importer vos informations dans **Gestionnaire de mots de passe Bitdefender**: <https://www.bitdefender.com/consumer/support/answer/2472/>

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.

3.2. Importation des données dans Password Manager

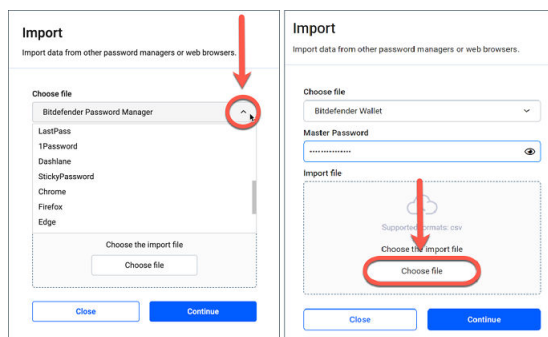
Bitdefender Password Manager vous permet d'importer facilement des mots de passe provenant de navigateurs ou d'autres gestionnaires. Si vous utilisiez déjà un autre service de gestion des mots de passe, vous y avez sans doute stocké beaucoup d'informations (noms d'utilisateur, mots de passe et autres 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 importer vos informations stockées à partir d'autres applications et navigateurs Web dans Bitdefender Password Manager, **quel que soit le système d'exploitation** sur lequel vous avez choisi d'installer ce produit :

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 gestionnaire de mots de passe ☰ menu pour développer la barre latérale sur la gauche et cliquez sur le ⚙️ **Paramètres** élément du menu.
3. Faites défiler jusqu'à **Données** section et cliquez sur le **Importer des données** option.
4. Utilisez le menu déroulant pour sélectionner le nom de l'application de gestion de mots de passe ou du navigateur à partir duquel vous souhaitez importer vos comptes. Entrez votre [Mot de passe maître](#) dans le champ correspondant, puis cliquez sur **Choisir le fichier**.



5. Parcourez vos dossiers pour trouver l'emplacement dans lequel vous avez enregistré le fichier contenant vos noms d'utilisateur et mots de passe, exporté depuis votre autre gestionnaire de mots de passe ou navigateur Web, puis appuyez 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.



3.3. 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

Un fichier CSV est **pas** crypté et contient des noms d'utilisateur et des mots de passe au format texte brut, ce qui signifie que vos informations privées peuvent être lues par toute personne ayant accès à votre appareil. Nous vous recommandons donc 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 du gestionnaire de mots de passe pour développer la barre latérale sur la gauche et cliquez sur le  **Paramètres** élément du menu.
3. Faites défiler jusqu'à **Données** section et cliquez sur le **Exporter des données** option.
4. Deux options vous sont alors proposées :
 - **CSV**
 - **Fichiers protégés par mot de passe**

Sélectionnez votre option préférée, puis saisissez votre mot de passe principal et cliquez sur le **Exporter des données** bouton.



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. Votre navigateur Web/application procédera en enregistrant un fichier nommé Bitdefender Password Manager_exported_data_current-date sur votre système dans le dossier de téléchargement par défaut. Il contient toutes vos 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.



3.4. Transfert de votre Bitdefender Wallet vers Password Manager

Parce que beaucoup de nos utilisateurs qui ont décidé d'adopter Bitdefender Password Manager comme service de gestion de mots de passe utilisaient auparavant notre fonctionnalité déjà existante **Bitdefender Wallet**, nous voulons montrer comment utiliser les données du portefeuille et transférer les informations d'identification de votre compte dans le nouveau produit amélioré Password Manager, ainsi que la synchronisation cloud des deux services.



Note

Notez que, comme Wallet est une fonctionnalité disponible uniquement sur les appareils Windows, ces instructions sont destinées uniquement aux systèmes d'exploitation Windows. Vous devez exporter la base de données Wallet et l'importer dans Password Manager **juste une fois**.

1. Exportation des mots de passe enregistrés depuis Wallet dans un fichier CSV:

- a. Après avoir mis à jour votre produit Bitdefender vers la dernière version et redémarré Windows, ouvrez le `C:\Program Files\Bitdefender\Bitdefender Security` dossier sur votre ordinateur, recherchez et double-cliquez sur le fichier nommé `bdwtxcon`.
- b. Ensuite, cliquez sur le **Commencez maintenant** sur l'écran d'accueil.
- c. Cochez la case à côté du nom du portefeuille que vous souhaitez exporter, puis cliquez sur le **Suivant** bouton. Si plusieurs portefeuilles sont sélectionnés, tous leurs mots de passe seront fusionnés dans un seul fichier.
- d. Entrez votre **Mot de passe maître** pour déverrouiller le portefeuille sélectionné à l'étape précédente, puis appuyez sur le **Ajouter un portefeuille** bouton.
- e. Une fois la base de données prête, un récapitulatif des comptes exportés depuis le Wallet s'affiche. Cliquez le **Sauvegardez vos données** bouton.
- f. Lorsque le système vous y invite, choisissez un nom pour le fichier CSV et enregistrez-le là où vous le retrouverez facilement (par



exemple sur votre bureau). Bitdefender exportera dans ce fichier toutes vos informations de connexion enregistrées.

2. Importation du fichier CSV exporté depuis Wallet vers Password Manager:

- a. Cliquez sur l'icône Password Manager dans la barre d'outils de votre navigateur. Saisissez votre mot de passe principal si nécessaire.
- b. Ouvrez le menu du gestionnaire de mots de passe ☰ pour développer le menu de la barre latérale sur la gauche et cliquez sur le ⚙️ **Paramètres** élément du menu.
- c. Faites défiler jusqu'à **Données** section et cliquez sur le **Importer des données** option.
- d. Sélectionner **Portefeuille Bitdefender** dans la liste des gestionnaires de mots de passe, saisissez votre **Mot de passe maître** dans le champ correspondant, puis cliquez sur **Choisir le fichier**.
- e. Sélectionnez le fichier CSV contenant vos identifiants et mots de passe exportés depuis le Wallet, puis appuyez sur **Continuer**.

3. Suppression du fichier CSV exporté depuis Wallet:

- a. Affichez votre solution de sécurité Bitdefender et accédez à **Confidentialité** sur le côté gauche de l'interface.
- b. Dans le **Password Manager** volet cliquez sur **Paramètres**.
- c. Cliquez sur l'onglet intitulé **Mes Wallets**.
- d. Au bas de la fenêtre, vous verrez une alerte vous informant des données non cryptées laissées sur votre ordinateur. Cliquez sur **Déchiqeter des fichiers**.
- e. Dans l'écran Destructeur de fichiers, appuyez sur **supprimer définitivement** et confirmez l'action.



4. CARACTÉRISTIQUES ET FONCTIONNALITÉS


Ce chapitre vous guidera à travers toutes les fonctions et fonctionnalités de Bitdefender Password Manager, en expliquant leur utilité et comment les utiliser le plus efficacement.

4.1. Gestion des mots de passe

4.1.1. 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 mot de passe** est accessible via l'onglet en haut de l'interface de Password Manager.

Le générateur peut être configuré pour renvoyer les mots de passe **entre 4 et 32 caractères**.

Vous pouvez également spécifier les types de caractères qui doivent ou non être présents dans le mot de passe généré aléatoirement en cochant ou décochant les cases correspondantes. (**minuscules, majuscules, chiffres, spécial**)

En appuyant sur le  à droite du mot de passe affiché, le générateur modifiera le mot de passe suggéré.

Pour utiliser le mot de passe affiché, appuyez sur **Utiliser le mot de passe**, action qui enregistrera la chaîne de caractères dans votre presse-papiers.



Note

Vos mots de passe précédemment générés seront temporairement stockés dans l'historique des mots de passe, accessible via le **Historique des mots de passe** bouton.







4.1.2. 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.

4.1.3. 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. Sous Windows ou macOS, cliquez sur le  **Gestionnaire de mots de passe** icône dans votre navigateur Web.
Sur Android ou iOS, lancez le  **Gestionnaire de mots de passe** 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. Ici, vous remarquerez un bouton affichant soit **Désactiver le remplissage automatique** ou **Activer le remplissage automatique**. Ce paramètre contrôle l'état de fonctionnement de la fonction de remplissage automatique intelligent.


4.1.4. 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 accéder au **Rapport de sécurité**, entrez dans l'interface du gestionnaire de mots de passe et sélectionnez son  bouton dans la barre supérieure.

4.1.5. 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 est également équipé d'un **mode hors-ligne** pour accéder à vos mots de passe, dans le cas où vous n'auriez pas accès à Internet. Cela rend vos mots de passe accessibles à tout moment et de n'importe où.

4.1.6. Suppression des mots de passe

Pour supprimer les mots de passe enregistrés, appuyez d'abord sur la  l'icône de modification à côté de l'entrée que vous souhaitez supprimer, située dans le  **Comptes** languette. Faites défiler vers le bas puis choisissez **Supprimer**. Lorsqu'on vous demande si vous êtes sûr de vouloir supprimer le compte, sélectionnez **Retirer**.

4.2. Gestion des comptes

4.2.1. Authentification





L'authentification dans Bitdefender Password Manager s'effectue via le **BROCHE** mis en place dans le processus d'installation du produit. (Notez que le **Verrouillage automatique** verrouillera le gestionnaire de mots de



passer ou se déconnectera après une période d'inactivité au niveau du navigateur ou la fermeture de l'application mobile)

De plus, cela peut également être fait grâce à l'utilisation de la biométrie, si disponible, comme **Empreinte digitale** ou **Déverrouillage par reconnaissance faciale**.

Pour **Activer ou désactiver** authentification basée sur la biométrie :

1. Sous Windows ou macOS, cliquez sur le  **Gestionnaire de mots de passe** icône dans votre navigateur Web.
Sur Android ou iOS, lancez le  **Gestionnaire de mots de passe** 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. Ici, vous remarquerez un bouton affichant soit **Désactiver la biométrie** ou **Activer la biométrie**. Ce paramètre contrôle l'état de fonctionnement de la fonction d'authentification basée sur la biométrie.


4.2.2. Réinitialisation du mot de passe principal



Important

Le **Modifier le mot de passe principal** la fonctionnalité n'est pas disponible sur les appareils mobiles. La seule façon de modifier ou de récupérer votre mot de passe principal est via l'extension de navigateur Bitdefender Password Manager sur un PC Windows ou un appareil macOS.



Voici comment changer votre **Mot de passe maître** par mesure de précaution et créez-en un nouveau dans Bitdefender Password Manager :

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



Important

Si vous ne vous souvenez pas du mot de passe principal actuel, cliquez sur le **J'ai oublié mon mot de passe** option sur le même écran. Entrer le **Clé de récupération à 24 chiffres** fourni lors de la configuration initiale de Bitdefender Password Manager, puis saisissez un nouveau mot de passe principal. **Si vous oubliez ou égarez** à la fois le **Mot de passe maître** et le **Clé de récupération**, en dernier recours, **contactez un représentant Bitdefender pour vous aider à réinitialiser votre compte**. La réinitialisation de votre compte entraînera **effacer toutes vos données et mots de passe** enregistré dans Bitdefender Password Manager.

3. 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.
4. Cliquez sur le **Mon compte** bouton dans le **Compte** section.
5. Une fenêtre contenant des informations sur votre abonnement à Password Manager s'affiche.
Cliquez sur le **Modifier le mot de passe principal** bouton.
6. 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.
7. appuie sur le **Changement** bouton lorsque vous avez terminé.
8. Patientez quelques instants pendant que Bitdefender réinitialise le mot de passe principal.
Ne fermez pas votre navigateur web !
9. Ensuite, vous recevez un nouveau **Clé de récupération à 24 chiffres**. Notez la clé de récupération dans un endroit sûr et **ne le perds pas**. Cette clé est le seul moyen d'accéder à vos mots de passe enregistrés dans Password Manager au cas où vous oublieriez le mot de passe principal.
Presse **Fermer** lorsque vous avez terminé.
10. Bitdefender Password Manager est alors déconnecté.
Pour déverrouiller le coffre-fort, utilisez le nouveau mot de passe principal que vous venez de définir.







4.3. Autres fonctionnalités

4.3.1. 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  **Gestionnaire de mots de passe** icône dans votre navigateur Web.
Sur Android ou iOS, lancez le  **Gestionnaire de mots de passe** 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  **Identities** élément du menu.
3. Appuyez sur le **Ajouter une identité** bouton en bas.
4. Complétez les détails que vous souhaitez enregistrer puis appuyez sur **Sauvegarder**.



4.3.2. 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  **Gestionnaire de mots de passe** icône dans votre navigateur Web.
Sur Android ou iOS, lancez le  **Gestionnaire de mots de passe** 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  **Cartes de crédit** élément du menu.
3. Appuyez sur le **Ajouter une identité** bouton en bas.
4. Complétez les détails que vous souhaitez enregistrer puis appuyez sur **Sauvegarder**.

4.3.3. 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  **Gestionnaire de mots de passe** icône dans votre navigateur Web.
Sur Android ou iOS, lancez le  **Gestionnaire de mots de passe** 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  **Sécurisez-moi** élément du menu.
3. Appuyez sur le **Sécurisez toutes les sessions** bouton.
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.

4.3.4. 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  **Gestionnaire de mots de passe** icône dans votre navigateur Web.



Sur Android ou iOS, lancez le  **Gestionnaire de mots de passe** 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  **Remarques** élément du menu.
3. Appuyez sur le  **Ajouter un commentaire** bouton.
Une fois que vous avez noté les informations que vous souhaitez conserver, appuyez sur **Sauvegarder**.



5. QUESTIONS FRÉQUEMMENT POSÉES

Certaines questions courantes concernant Bitdefender Password Manager ont tendance à se répéter. Nous avons les réponses ! Ici, vous pouvez en savoir plus sur votre compte Bitdefender, l'importation de mots de passe, les protocoles de sécurité des données et d'autres sujets importants pour nos clients.

Questions générales sur Bitdefender Password Manager

Comment arrêter la fenêtre contextuelle Password Manager dans ma solution de sécurité Bitdefender ?

La notification du gestionnaire de mots de passe affichée par Bitdefender Total Security, Internet Security et Antivirus Plus en août 2022 peut être ignorée en cliquant sur le bouton « x ». La fenêtre "Gérer vos mots de passe avec Bitdefender Password Manager" réapparaîtra au hasard plusieurs fois avant de disparaître définitivement. Vous pouvez désactiver ce message promotionnel en basculant **Avis de recommandation** en position désactivée dans les paramètres de Bitdefender.

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

Une fois que votre abonnement à Password Manager expire et n'est plus actif, vous disposez d'un maximum de 90 jours pour exporter vos mots de passe. Vos mots de passe seront sauvegardés pendant 30 jours supplémentaires. Pendant ces 90 jours, vous ne pourrez exporter que vos données. Vous ne pouvez pas continuer à utiliser Password Manager. La fonction de remplissage automatique cessera de fonctionner, ainsi que la possibilité de générer des mots de passe.

À la fin de la période de grâce de 90 jours, vous disposez de 30 jours supplémentaires pour contacter le support Bitdefender et demander la restauration de vos mots de passe dans la base de données en direct. Vous pourrez alors exporter vos mots de passe depuis Bitdefender Password Manager.

Vos données seront conservées dans la base de données en direct uniquement jusqu'à la fin de la journée où elles ont été restaurées à la demande. À minuit, la base de données est effacée - et si vous n'avez pas encore dépassé la période supplémentaire de 30 jours, les mots de passe



peuvent être restaurés à nouveau à partir de la sauvegarde. Les données brutes de la base de données de la sauvegarde peuvent être fournies sur demande à l'utilisateur, mais la base de données est cryptée et les informations ne sont pas accessibles.

Qu'est-ce qu'un mot de passe maître et pourquoi dois-je m'en souvenir ?

Le mot de passe principal est la clé qui ouvre la porte à tous les mots de passe stockés dans votre compte Bitdefender Password Manager. Le mot de passe principal doit comporter au moins 8 caractères. Créez donc un mot de passe principal fort, mémorisez-le et ne le partagez jamais avec qui que ce soit. Pour créer un mot de passe principal fort, nous vous recommandons d'utiliser une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux (comme #, \$ ou @).

Comment puis-je empêcher Bitdefender de demander mon mot de passe maître à chaque fois que j'ouvre le navigateur ?

Si vous verrouillez votre appareil sans fermer votre navigateur, le gestionnaire de mots de passe ne se verrouille pas et vous pouvez accéder à vos données à votre retour. Par mesure de sécurité, chaque fois que vous ouvrez le navigateur, vous devez vous connecter avec votre compte Bitdefender Central, puis saisir votre mot de passe principal.

- ☐ Pour arrêter l'invite de connexion centrale, accédez à ⚙ Paramètres et cochez "Désactiver l'onglet de connexion au démarrage".
- ☐ Pour arrêter l'invite du mot de passe principal, cochez la case "Se souvenir de moi" sur l'écran Déverrouillez votre coffre-fort.

Pourquoi ne stockez-vous pas mon mot de passe principal, et que se passe-t-il si je l'oublie ?

La raison pour laquelle nous ne stockons pas votre mot de passe principal sur nos serveurs est que vous seul pouvez accéder à votre compte. C'est le moyen le plus sûr. Si Bitdefender Password Manager ne reconnaît pas votre mot de passe principal, assurez-vous de le saisir correctement et que la touche de verrouillage des majuscules n'est pas active sur le clavier.

Si vous oubliez le mot de passe principal, vous pouvez toujours utiliser la clé de récupération pour déverrouiller Password Manager. Pendant le processus d'inscription, Bitdefender Password Manager fournit un **clé de récupération** qui peuvent être utilisés pour retrouver l'accès au compte sans perdre vos données.



Si vous oubliez ou égarez à la fois le mot de passe principal et la clé de récupération, en dernier recours, contactez un représentant Bitdefender pour réinitialiser votre compte.



Important

La réinitialisation de votre compte effacera toutes vos données et mots de passe enregistrés dans Bitdefender Password Manager.

Plusieurs utilisateurs peuvent-ils partager un abonnement Bitdefender Password Manager ?

Pour l'instant, la possibilité d'avoir plusieurs utilisateurs sur le même abonnement à Password Manager n'est pas disponible, mais nous travaillons à l'activation de cette fonctionnalité dans un avenir proche.

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

Le mode hors ligne est automatiquement activé lorsque la connexion Internet est interrompue lors de l'utilisation de Bitdefender Password Manager. Si vous êtes déjà connecté et que vous avez entré votre mot de passe principal, le mode hors ligne vous permet d'accéder à vos mots de passe lorsqu'une connexion Internet est hors de portée.

Comment désinstaller Bitdefender Password Manager ?

Pour désinstaller Bitdefender Password Manager :

- Sous Windows et macOS :
Supprimez l'extension Password Manager de votre navigateur Web. Faites un clic droit sur l'icône Bitdefender et sélectionnez « Supprimer ».
- Sur Android :
Appuyez et maintenez l'application Password Manager, puis faites-la glisser vers le haut de l'écran où il est écrit "Désinstaller".
- Sur iOS et iPadOS :
Appuyez et maintenez l'application Password Manager jusqu'à ce que toutes les applications sur votre écran commencent à bouger, puis appuyez sur le X en haut à gauche de l'icône Bitdefender.

Questions de confidentialité et de sécurité sur Bitdefender Password Manager

Les employés de Bitdefender pourraient-ils voir mes mots de passe ?



Absolument pas. Votre vie privée est notre priorité absolue. C'est la raison principale pour laquelle nous ne stockons pas votre mot de passe maître sur nos serveurs de données : afin que personne n'ait accès à votre compte, pas même les employés de l'entreprise. Chaque mot de passe et compte sont hautement cryptés avec l'algorithme de sécurité des données le plus puissant, et le code que nous voyons ressemble simplement à une chaîne aléatoire de chiffres et de lettres mélangés.

Que se passerait-il si les serveurs de Password Manager étaient piratés ?

Chaque mot de passe est crypté localement sur votre appareil avant qu'il ne s'approche de nos serveurs, donc si des pirates venaient à s'introduire dans notre système, ils n'obtiendraient que des pages de lettres et de chiffres aléatoires sans votre clé pour les décrypter. Cela signifie que vous et les détails de votre compte êtes toujours en sécurité avec nous.



6. OBTENIR DE L'AIDE

6.1. 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.

Si vous ne trouvez pas de réponse à votre question dans les ressources fournies, n'hésitez pas à nous contacter ici :

<https://www.bitdefender.com/consumer/support/help/>

6.2. 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.com/support/consumer.html>
- Communauté des experts Bitdefender :
<https://community.bitdefender.com>
- 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.

6.2.1. 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, des rapports sur les incidents et les bugs constatés par les techniciens et les développeurs de Bitdefender. Vous y découvrirez aussi, entre autres, des articles généraux sur la



prévention contre les menaces et sur la gestion des solutions Bitdefender, comprenant des explications précises.

La base de connaissances de Bitdefender est ouverte au public et consultable gratuitement. C'est un autre moyen de fournir aux clients de Bitdefender les informations techniques dont ils ont besoin. Toutes les demandes d'information valides ou les rapports sur les bugs observés par des clients de Bitdefender finissent dans cette base de données de Bitdefender, de même que les rapports sur les incidents, les travaux associés, les aide-mémoire ou les articles d'information venant compléter les fichiers d'aide sur chaque produit.

Le Centre de Support Bitdefender est disponible à tout moment à l'adresse suivante: <https://www.bitdefender.com/support/consumer.html>.

6.2.2. 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 conviviale dans laquelle tous les utilisateurs peuvent trouver de l'aide.

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>

6.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia regroupe toutes les dernières informations sur les cybermenaces. c'est là que les experts Bitdefender partagent deq



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/>.



6.3. Pour nous joindre

Une communication efficace est la clé d'une entreprise prospère. Depuis 2001, BITDEFENDER s'est forgé une réputation incontestable en recherchant constamment une meilleure communication afin de dépasser les attentes de nos clients et partenaires. Si vous avez des questions, n'hésitez pas à nous contacter directement via notre [Centre de support Bitdefender \(page 34\)](#).

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



GLOSSAIRE

Code d'activation

Il s'agit d'une clé unique qui peut être achetée dans le commerce et utilisée pour activer un produit ou un service spécifique. Un code d'activation permet l'activation d'un abonnement valide pour une certaine période de temps et de nombre d'appareils et peut également être utilisé pour prolonger un abonnement avec la condition à générer 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 avec Microsoft Internet Explorer pour créer des pages Web interactives qui ressemblent et se comportent comme des programmes informatiques, plutôt que comme des pages statiques. Avec ActiveX, les utilisateurs peuvent poser ou répondre à des questions, utiliser des boutons-poussoirs et interagir d'autres manières avec la page Web. Les contrôles ActiveX sont souvent écrits à l'aide de Visual Basic. Active X se distingue par une absence totale de contrôles de sécurité ; les experts en sécurité informatique déconseillent son utilisation sur Internet.

Menace persistante avancée

La menace persistante avancée (APT) exploite les vulnérabilités des systèmes pour voler des informations importantes afin de les transmettre à la source. Les grands groupes tels que les organisations, les entreprises ou les gouvernements sont ciblés par cette menace. L'objectif d'une menace persistante avancée est de rester longtemps non détectée en étant capable de surveiller et de collecter des informations importantes sans endommager les machines ciblées. La méthode utilisée pour injecter la menace dans le réseau consiste à utiliser un fichier PDF ou un document Office qui semble inoffensif afin que chaque utilisateur puisse exécuter les fichiers.

Adware

L'adware est souvent associé à une application hôte qui est fournie gratuitement tant que l'utilisateur accepte d'accepter l'adware. Étant donné que les applications publicitaires sont généralement installées



après que l'utilisateur a accepté un accord de licence indiquant l'objectif de l'application, aucune infraction n'est commise. Cependant, les publicités contextuelles peuvent devenir gênantes et, dans certains cas, dégrader les performances du système. De plus, les informations que certaines de ces applications collectent peuvent poser des problèmes de confidentialité pour les utilisateurs qui n'étaient pas pleinement conscients des termes du contrat de licence.

Archive

Disquette, bande ou répertoire qui contient des fichiers qui ont été sauvegardés.

Fichier contenant un ou plusieurs fichiers dans un format compressé.

Porte arrière

Un trou dans la sécurité d'un système délibérément laissé en place par les concepteurs ou les mainteneurs. La motivation de tels trous n'est pas toujours sinistre ; certains systèmes d'exploitation, par exemple, sont livrés prêts à l'emploi avec des comptes privilégiés destinés à être utilisés par les techniciens de service sur le terrain ou les programmeurs de maintenance du fournisseur.

Secteur de démarrage

Un secteur au début de chaque disque qui identifie l'architecture du disque (taille de secteur, taille de cluster, etc.). Pour les disques de démarrage, le secteur de démarrage contient également un programme qui charge le système d'exploitation.

Virus de démarrage

Menace qui infecte le secteur d'amorçage d'une disquette fixe ou d'une disquette. Une tentative d'amorçage à partir d'une disquette infectée par un virus de secteur d'amorçage entraînera l'activation de la menace en mémoire. Chaque fois que vous démarrerez votre système à partir de ce moment, la menace sera active en mémoire.

Réseau de zombies

Le terme « botnet » est composé des mots « robot » et « réseau ». Les botnets sont des appareils connectés à Internet infectés par des menaces et peuvent être utilisés pour envoyer des spams, voler des données, contrôler à distance des appareils vulnérables ou propager des logiciels espions, des rançongiciels et d'autres types de menaces. Leur objectif



est d'infecter autant d'appareils connectés que possible, tels que des PC, des serveurs, des appareils mobiles ou IoT appartenant à de grandes entreprises ou industries.

Navigateur

Abréviation de navigateur Web, une application logicielle utilisée pour localiser et afficher des pages Web. Les navigateurs populaires incluent Microsoft Internet Explorer, Mozilla Firefox et Google Chrome. Ce sont des navigateurs graphiques, ce qui signifie qu'ils peuvent afficher des graphiques ainsi que du texte. De plus, la plupart des navigateurs modernes peuvent présenter des informations multimédias, y compris le son et la vidéo, bien qu'ils nécessitent des plug-ins pour certains formats.

Attaque de force brute

Attaque de devinette de mot de passe utilisée pour s'introduire dans un système informatique en saisissant des combinaisons de mots de passe possibles, en commençant généralement par le mot de passe le plus facile à deviner.

Ligne de commande

Dans une interface de ligne de commande, l'utilisateur tape des commandes dans l'espace prévu directement sur l'écran en utilisant le langage de commande.

Biscuits

Dans l'industrie Internet, les cookies sont décrits comme de petits fichiers contenant des informations sur des ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs pour suivre vos intérêts et vos goûts en ligne. Dans ce domaine, la technologie des cookies est toujours en cours de développement et l'intention est de cibler les publicités directement sur ce que vous avez déclaré être vos intérêts. C'est une épée à double tranchant pour beaucoup de gens parce que d'une part, c'est efficace et pertinent car vous ne voyez que des publicités sur ce qui vous intéresse. D'autre part, cela implique en fait de « suivre » et de « suivre » où vous allez et sur quoi vous cliquez. Naturellement, il y a un débat sur la confidentialité et de nombreuses personnes se sentent offensées par l'idée qu'elles sont considérées comme un "numéro SKU" (vous savez, le code-barres au dos des emballages qui est scanné à la caisse de l'épicerie) . Bien que ce point de vue puisse être extrême, dans certains cas, il est exact.

Harcèlement sur internet



Lorsque des pairs ou des étrangers commettent des actes abusifs contre des enfants dans le but de les blesser physiquement. Pour nuire émotionnellement, les agresseurs envoient des messages méchants ou des photos peu flatteuses, ce qui isole leurs victimes des autres ou les frustre.

Dictionnaire Attaque

Attaques de devinettes de mot de passe utilisées pour s'introduire dans un système informatique en saisissant une combinaison de mots courants pour générer des mots de passe potentiels. La même méthode est utilisée pour deviner les clés de déchiffrement des messages ou documents chiffrés. Les attaques par dictionnaire réussissent parce que de nombreuses personnes ont tendance à choisir des mots de passe courts et simples faciles à deviner.

Disque

C'est une machine qui lit et écrit des données sur un disque. Un disque dur lit et écrit sur les disques durs. Un lecteur de disquettes accède aux disquettes. Les lecteurs de disque peuvent être internes (logés dans un ordinateur) ou externes (logés dans un boîtier séparé qui se connecte à l'ordinateur).

Télécharger

Pour copier des données (généralement un fichier entier) d'une source principale vers un périphérique. Le terme est souvent utilisé pour décrire le processus de copie d'un fichier d'un service en ligne vers son propre ordinateur. Le téléchargement peut également faire référence à la copie d'un fichier d'un serveur de fichiers réseau vers un ordinateur du réseau.

E-mail

Courrier électronique. Service qui envoie des messages sur des ordinateurs via des réseaux locaux ou mondiaux.

Événements

Une action ou un événement détecté par un programme. Les événements peuvent être des actions de l'utilisateur, telles que cliquer sur un bouton de la souris ou appuyer sur une touche, ou des occurrences du système, telles que le manque de mémoire.

Exploits



Un moyen de tirer parti des différents bogues ou vulnérabilités présents dans un ordinateur (logiciel ou matériel). Ainsi, les pirates peuvent prendre le contrôle d'ordinateurs ou de réseaux.

Faux positif

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

Extension de nom de fichier

La partie d'un nom de fichier, après le dernier point, qui indique le type de données stockées dans le fichier. De nombreux systèmes d'exploitation utilisent des extensions de nom de fichier, par exemple Unix, VMS et MS-DOS. Ils sont généralement d'une à trois lettres (certains anciens systèmes d'exploitation tristes n'en supportent pas plus de trois). Les exemples incluent "c" pour le code source C, "ps" pour PostScript, "txt" pour du texte arbitraire.

Heuristique

Une méthode basée sur des règles pour identifier les nouvelles menaces. Cette méthode d'analyse ne repose pas sur une base de données d'informations sur les menaces spécifiques. L'avantage du scan heuristique est qu'il n'est pas dupe d'une nouvelle variante d'une menace existante. Cependant, il peut occasionnellement signaler un code suspect dans des programmes normaux, générant ce que l'on appelle des "faux positifs".

Pot de miel

Un système informatique leurre destiné à attirer les pirates pour étudier leur façon d'agir et identifier les méthodes hérétiques qu'ils utilisent pour collecter des informations système. Les entreprises et les sociétés sont plus intéressées par la mise en œuvre et l'utilisation de pots de miel pour améliorer leur état général de sécurité.

IP

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

Applet Java

Programme Java conçu pour s'exécuter uniquement sur une page Web. Pour utiliser une applet sur une page Web, vous devez spécifier le nom



de l'applet et la taille (longueur et largeur, en pixels) que l'applet peut utiliser. Lors de l'accès à la page Web, le navigateur télécharge l'applet à partir d'un serveur et l'exécute sur la machine de l'utilisateur (le client). Les applets diffèrent des applications en ce sens qu'elles sont régies par un protocole de sécurité strict.

Par exemple, même si les applets s'exécutent sur le client, elles ne peuvent ni lire ni écrire de données sur la machine du client. De plus, les applets sont encore plus restreintes afin qu'elles ne puissent lire et écrire que des données du même domaine à partir duquel elles sont servies.

Enregistreur de frappe

Un enregistreur de frappe est une application qui enregistre tout ce que vous tapez. Les enregistreurs de frappe ne sont pas de nature malveillante. Ils peuvent être utilisés à des fins légitimes, telles que la surveillance des employés ou des activités des enfants. Cependant, ils sont de plus en plus utilisés par les cybercriminels à des fins malveillantes (par exemple, pour collecter des données privées, telles que des identifiants de connexion et des numéros de sécurité sociale).

Macro-virus

Type de menace informatique codée sous forme de macro intégrée dans un document. De nombreuses applications, telles que Microsoft Word et Excel, prennent en charge de puissants langages de macro. Ces applications vous permettent d'intégrer une macro dans un document et d'exécuter la macro à chaque ouverture du document.

Client de messagerie

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

Mémoire

Zones de stockage internes de l'ordinateur. Le terme mémoire identifie le stockage de données qui se présente sous la forme de puces, et le mot stockage est utilisé pour la mémoire qui existe sur des bandes ou des disques. Chaque ordinateur est livré avec une certaine quantité de mémoire physique, généralement appelée mémoire principale ou RAM.

Non heuristique

Cette méthode d'analyse repose sur une base de données d'informations sur les menaces spécifiques. L'avantage de l'analyse non heuristique est



qu'elle n'est pas dupe de ce qui pourrait sembler être une menace et ne génère pas de fausses alarmes.

Prédateurs en ligne

Les personnes qui cherchent à attirer des mineurs ou des adolescents dans des conversations dans le but de les impliquer dans des activités sexuelles illégales. Les réseaux sociaux sont l'endroit idéal où les enfants vulnérables peuvent facilement être chassés et séduits pour qu'ils commettent des activités sexuelles, en ligne ou en face à face.

Programmes emballés

Un fichier dans un format de compression. De nombreux systèmes d'exploitation et applications contiennent des commandes qui vous permettent de compresser un fichier afin qu'il occupe moins de mémoire. Par exemple, supposons que vous disposiez d'un fichier texte contenant dix espaces consécutifs. Normalement, cela nécessiterait dix octets de stockage.

Cependant, un programme qui compresse les fichiers remplacerait les caractères d'espacement par un caractère spécial de série d'espaces suivi du nombre d'espaces remplacés. Dans ce cas, les dix espaces ne nécessiteraient que deux octets. Ce n'est qu'une technique d'emballage - il y en a beaucoup d'autres.

Chemin

Les directions exactes vers un fichier sur un ordinateur. Ces directions sont généralement décrites au moyen du système de classement hiérarchique de haut en bas.

L'itinéraire entre deux points quelconques, comme le canal de communication entre deux ordinateurs.

Hameçonnage

Le fait d'envoyer un e-mail à un utilisateur prétendant à tort être une entreprise légitime établie dans le but d'escroquer l'utilisateur pour qu'il restitue des informations privées qui seront utilisées pour le vol d'identité. L'e-mail invite l'utilisateur à visiter un site Web où il lui est demandé de mettre à jour des informations personnelles, telles que des mots de passe et des numéros de carte de crédit, de sécurité sociale et de compte bancaire, que l'organisation légitime possède déjà. Le site Web, cependant, est faux et configuré uniquement pour voler les informations de l'utilisateur.



Photon

Technologie Bitdefender, innovante et discrète, conçue pour limiter l'impact de la solution de sécurité sur les performances. En surveillant l'activité de votre ordinateur en arrière-plan, elle crée des modèles d'utilisation qui aident à optimiser les processus de démarrage et d'analyse.

Virus polymorphe

Menace qui change de forme pour chaque fichier qu'elle infecte. Puisqu'elle n'a pas de forme unique bien définie, elle est plus difficile à identifier.

Port

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

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

Logiciels de rançon

Programme malveillant qui tente 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 les e-mails, 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 à l'origine de ces logiciels malveillants.

Fichier de rapport

Fichier qui enregistre les actions qui surviennent. Bitdefender tient à jour un fichier de rapport contenant les chemins analysés, les dossiers, le nombre d'archives et de fichiers analysés, le nombre de fichiers suspects et infectés.

Rootkit



Ensemble d'outils logiciels permettant aux administrateurs d'accéder à un système. Le terme a été utilisé initialement pour les systèmes d'exploitation UNIX et désignait alors des outils recompilés fournissant des droits administrateurs intrusifs, permettant de cacher leur présence aux administrateurs système.

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

Les rootkits ne sont pas nécessairement malveillants. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des rootkits. 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 rootkits pirates sont une menace importante pour l'intégrité et la sécurité d'un système. Ils peuvent analyser le trafic, ouvrir des portes dérobées, 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 peuvent être exécutées sans intervention de l'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 spywares sont généralement cachés dans des sharewares et des logiciels gratuits pouvant être téléchargés sur Internet. Notons toutefois que la plupart des sharewares et des logiciels gratuits ne contiennent pas de spywares. Une fois installé, le spyware surveille l'activité de l'utilisateur sur internet et transmet discrètement ces informations à une tierce personne. Les spywares peuvent également récupérer des adresses e-mail, des mots de passe ou même des 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. Le mode d'infection le plus fréquent est le téléchargement de logiciels de partage de fichiers (peer-to-peer).



Sans parler des questions d'éthique et de respect de la vie privée, les spywares épuisent 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 arrière-plan 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 lui-même.

Abonnement

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 peut être renouvelé automatiquement en utilisant les informations données par l'utilisateur lors du premier achat.

Barre d'état système

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 individus malveillants. Une menace simple peut se copier très



rapidement et sans arrêt et est relativement facile à créer. Même une menace simple 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

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

Troyen

Programme destructeur qui se fait passer pour 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 aussi destructeurs. L'un des types les plus pernicieux 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 légende de l'Illiade écrite par Homère, dans laquelle les Grecs offrent à leurs ennemis, les Troyens, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur ville qu'ils se rendent compte que celui-ci est plein de soldats grecs, qui ouvrent les portes de la ville à leurs troupes et entraînent ainsi la chute de Troie.

Mise à jour

Nouvelle version du logiciel ou d'un élément matériel, destinée à remplacer une ancienne version du même produit. En général, les mises à jour ne se font que si une ancienne version du produit est déjà installée sur votre appareil.

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

Réseau privé virtuel (VPN)

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



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.