GUIDE D'UTILISATION

Bitdefender CONSUMER SOLUTIONS

SecurePass

Bitdefender SecurePass

Guide de l'utilisateur

Publication date 20/11/2024

Mention légale

Bitdefender

Table des matières

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 SecurePass 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 SecurePass.

Importation et exportation de vos mots de passe (page 11)

Découvrez comment importer ou exporter des mots de passe depuis et vers SecurePass.

Caractéristiques et fonctionnalités (page 15)

Utilisation de Bitdefender SecurePass et de toutes ses fonctionnalités.

Obtenir de l’aide (page 28)

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.
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.
Nom de fichier	Les noms de fichiers et de répertoires sont écrits dans une police à espacement fixe.
Option	Toutes les options du produit sont écrites en caractères **gras**.
Mot-clé	Les mots-clés et les expressions importantes sont mis en évidence à l'aide de caractères **gras**.

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. 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 SECUREPASSQUE

Bitdefender SecurePass 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 SecurePass 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. 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 SecurePass uniquement sur les appareils fonctionnant avec les systèmes d'exploitation suivants :

- **Pour les utilisateurs d'appareils Windows :**
  - Windows 7 avec Service Pack 1
  - Windows 8.1
  - 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 SecurePass 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 SecurePass ne pourra pas être installé ou ne fonctionnera pas correctement.

2.2. Installation

Ce chapitre explique comment installer Bitdefender SecurePass 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**.

- **Google Chrome**
- **Mozilla Firefox**
- **Microsoft Edge**
- **Safari**

Pour installer Bitdefender SecurePass :

1. Après avoir acheté Bitdefender SecurePass, suivez les étapes indiquées dans l'e-mail de confirmation afin d'activer votre abonnement.
2. Connectez-vous à Bitdefender Central à l'aide de vos informations d'identification.
   Dans le menu de gauche, sélectionnez **Pass sécurisé**.
3. Dans le panneau SecurePass, sélectionnez votre navigateur préféré.
4. Installez l'extension de navigateur :
   - **Google Chrome :**
     a. Cliquez sur **Ajouter à Chrome** bouton.
     b. Dans la boîte de confirmation, cliquez sur **Ajouter une extension**.
   - **Mozilla Firefox :**
     a. Cliquez sur **Ajouter à Firefox** bouton.
     b. Cliquez sur **Installer** bouton situé dans le coin supérieur droit de l'écran.
   - **Microsoft Edge :**
     a. Cliquez sur **Obtenez** bouton.
     b. Cliquez **Ajouter une extension** dans l'invite qui s'affiche.
   - **Safari :**

a. Le programme d'installation de SecurePass sera téléchargé sur votre appareil macOS. Double-cliquez sur le fichier téléchargé et suivez les instructions qui s'affichent à l'écran

b. À la fin du processus d'installation, ouvrez **Safari** navigateur et sélectionnez **Préférences** dans la barre de menu supérieure.

c. Dans la fenêtre Préférences, cliquez sur **Onglet Extensions**.

d. Cochez la case à côté de **Bitdefender SecurePass** pour l'activer.

Une fois l'extension installée, vous pouvez passer à Processus de configuration (page 9).

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.

1. Avant toute chose, après l'achat, assurez-vous d'ouvrir l'e-mail de confirmation que vous avez reçu afin de suivre les instructions qui y sont fournies pour activer votre abonnement SecurePass.
2. Ouvrez le Google Play Store sur votre appareil Android.
3. Dans la barre de recherche du Google Play Store, tapez **Bitdefender SecurePass**, localisez et téléchargez l'application.
4. Une fois le téléchargement terminé, ouvrez l'application et, si nécessaire, suivez les étapes de configuration à l'écran nécessaires pour terminer le processus d'installation.

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.

1. Avant toute chose, après l'achat, assurez-vous d'ouvrir l'e-mail de confirmation que vous avez reçu afin de suivre les instructions qui y sont fournies pour activer votre abonnement SecurePass.

2. Ouvrez l'App Store sur votre appareil iOS.
3. Dans la barre de recherche de l'App Store, tapez **Bitdefender SecurePass**, localisez et téléchargez l'application.
4. Une fois le téléchargement terminé, ouvrez l'application et, si nécessaire, suivez les étapes de configuration à l'écran nécessaires pour terminer le processus d'installation.

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

2.3. Processus de configuration

Pour configurer Bitdefender SecurePass sur votre navigateur/appareil mobile :

1. Une fois le processus d'installation terminé, ouvrez l'extension/ l'application SecurePass et connectez-vous.
   Utilisez les informations d'identification du compte Bitdefender associé à votre abonnement SecurePass.
2. Vous serez invité à créer un **Mot de passe principal**.

   > **Important**
   > Notez que vous aurez besoin de ce mot de passe principal pour déverrouiller tous les mots de passe, informations de carte de crédit et notes enregistrés dans Bitdefender SecurePass. Il s'agit essentiellement de la clé qui permet au propriétaire d'utiliser ce produit.

   Assurez-vous de saisir un mot de passe principal fort sans risquer de l'oublier facilement.
   Une fois que vous avez choisi un mot de passe principal fort et unique, cliquez sur **Enregistrer et continuer**.
3. Ensuite, vous recevrez un **Clé de récupération**.

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** configuré précédemment pour votre compte.

- Enregistrez la clé de restauration en la copiant dans votre presse-papiers ou en la téléchargeant au format PDF.
  Vous pouvez appuyer sur **Fermer** une fois terminé.

4. Une fois terminé, sélectionnez **Accédez à votre coffre-fort** bouton.

Maintenant que le processus de configuration est terminé, vous pouvez commencer à utiliser Bitdefender SecurePass.

3. 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.

3.1. Compatibilité

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

- Gestionnaire de mots de passe Bitdefender
- Portefeuille Bitdefender
- Bitdefender SecurePass
- Pass sécurisé
- 1 mot de passe
- Kaspersky
- Dashlane
- Navigateur Chrome
- Navigateur Firefox
- Microsoft Edge
- Bitwarden
- Dernier Pass
- KeePass
- RoboForm

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 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. Ouvrez Bitdefender SecurePass et accédez à **Réglages**.
   - Dans le navigateur :
     Cliquez sur **Réglages** dans le coin supérieur droit de la page.
   - Dans l'application :
     Appuyez sur **Plus** bouton dans le coin inférieur droit de l'écran et, en haut de la liste qui apparaît ensuite, appuyez sur **Réglages**.
2. Dans le **Sauvegarde et restauration** section, sélectionnez **Importer des mots de**. La fenêtre d'importation s'ouvre.
3. Sélectionnez le nom du gestionnaire de mots de passe ou du navigateur Web que vous avez utilisé auparavant dans le menu déroulant accessible via **Sélectionnez le type de fichier** champ.

   > **Remarque**
   > Si un mot de passe a été utilisé pour crypter le fichier, vous devrez le saisir dans **Mot de passe** champ ; sinon, vous pouvez le laisser vide.

4. Sélectionnez le **Sélectionnez le fichier à importer** déposé.
   Accédez à l'emplacement où les données exportées appartenant à votre ancien gestionnaire de mots de passe ont été enregistrées.

Choisissez le fichier une fois que vous l'avez trouvé, puis cliquez sur **Ouvrir**.

5. Après avoir sélectionné le fichier, sélectionnez **Importer** dans le coin inférieur gauche de la fenêtre d'importation. Le processus débutera sous peu, accompagné d'une barre de progression.

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.

> **Remarque**
> En retournant dans votre coffre-fort de mots de passe dans SecurePass, vous remarquerez un dossier nommé **Importer**, contenant toutes les données de votre ancien gestionnaire de mots de passe ou navigateur Web.

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**
> 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. Ouvrez Bitdefender SecurePass et accédez à **Réglages**.
   - Dans le navigateur :
     Cliquez sur **Réglages** dans le coin supérieur droit de la page.
   - Dans l'application :

Appuyez sur **Plus** bouton dans le coin inférieur droit de l'écran et, en haut de la liste qui apparaît ensuite, appuyez sur **Réglages**.

2. Dans le **Sauvegarde et restauration** section, sélectionnez **Exporter les mots de**. La fenêtre d'exportation s'ouvre.
3. Cliquez sur **Sélectionnez le type de fichier**. Dans le menu déroulant, choisissez d'exporter vos données au format JSON ou au format CSV. Vous pouvez également saisir un mot de passe pour protéger le fichier exporté.
   Cochez la case correspondante si vous souhaitez également inclure des éléments partagés.
4. Cliquez **Exporter** dans le coin inférieur gauche de la fenêtre d'exportation et enregistrez le fichier exporté sur votre appareil.

4. 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.

4.1. Enregistrer manuellement les mots de passe

Vous pouvez stocker en toute sécurité des informations telles que des mots de passe, des informations d'identification et autres, telles que des informations de carte de crédit ou des notes dans Bitdefender SecurePass manuellement, de la manière suivante :

1. Ouvrez Bitdefender SecurePass
2. Dans le **Mon coffre-fort** onglet, appuyez sur **+Ajouter un article** bouton.
3. Sélectionnez le type d'article que vous souhaitez ajouter. (compte, carte de crédit, identité ou note).
4. Renseignez les champs obligatoires en fonction de l'élément sélectionné.
5. Après avoir renseigné toutes les informations nécessaires, enregistrez l'article afin de l'ajouter à votre coffre-fort SecurePass.

4.2. Générateur de mots de passe

Bitdefender SecurePass inclut une fonctionnalité de génération de mot de passe qui peut vous aider à créer des mots de passe sécurisés.

Pour accéder au générateur de mots de passe et l'utiliser :

1. Ouvrez Bitdefender SecurePass et accédez au **Générer mot de passe** onglet sur le côté gauche de l'écran. Vous serez alors redirigé vers le générateur de mots de passe intégré à SecurePass
2. Personnalisez le mot de passe que vous êtes sur le point de générer en fonction de vos besoins et préférences.
   - Longueur du mot de passe : faites glisser le curseur pour déterminer une longueur comprise entre 8 et 32 caractères.

- Lettres majuscules/minuscules : sélectionnez le type de lettres que vous souhaitez ajouter (ou les deux) en fonction du niveau de complexité de votre mot de passe.
- Chiffres : si vous cochez cette case, des chiffres seront inclus dans la chaîne de caractères qui constitue votre mot de passe.
- Caractères spéciaux : ajoutez des symboles à votre mot de passe pour en améliorer la complexité.

> **Remarque**
> Appuyez sur **Enregistrer les paramètres** bouton permettant à SecurePass de les mémoriser et de toujours générer des mots de passe en fonction des paramètres que vous avez enregistrés.

3. Générez un nouveau mot de passe en cliquant sur l'icône en forme de flèche circulaire située sous le mot de passe actuellement affiché. Chaque clic génère une nouvelle chaîne de caractères.
4. Une fois satisfait du mot de passe généré, vous pouvez soit le copier dans votre presse-papiers, soit cliquer sur **Enregistrer le compte** bouton pour le stocker dans votre coffre-fort (en l'associant à d'autres informations de compte).

> **Remarque**
> Vous pouvez également générer rapidement un mot de passe **directement à partir des formulaires d'inscription** en cliquant sur l'icône Bitdefender SecurePass présente dans le champ du mot de passe de la page d'inscription. En cliquant dessus, vous pouvez ensuite choisir **Générer mot de passe** option.

4.3. Vérification de la solidité du mot de

Bitdefender SecurePass offre la possibilité d'évaluer le niveau de sécurité des mots de passe enregistrés et des données sensibles. Il s'agit d'une fonctionnalité essentielle pour évaluer et évaluer toute vulnérabilité potentielle en matière de confidentialité et de sécurité de vos données.

Pour vérifier le niveau de sécurité des mots de passe enregistrés :

1. Ouvrez Bitdefender SecurePass et, dans le menu de messagerie, sélectionnez **Rapport de sécurité** onglet.

L'onglet Rapport de sécurité est divisé en quatre sections : piraté, faible, ancien et dupliqué.

2. Le nombre de mots de passe appartenant à chacune des quatre catégories sera affiché à l'écran.
   De plus, en parcourant la liste des mots de passe stockés, chaque mot de passe sera étiqueté avec la catégorie dans laquelle il se trouve.

Afin de comprendre la signification de ces niveaux de sécurité, voici quelques brèves informations sur chacun d'entre eux :

- Mots de passe piratés : si l'une de vos informations d'identification a fait l'objet d'une violation de données, elle sera répertoriée dans **violée** section.

  > **Remarque**
  > Pour vérifier si l'un de vos mots de passe a été compromis ou a été divulgué à la suite de violations de données, cliquez sur **Exécuter une analyse de sécurité** bouton.

- Mots de passe faibles : SecurePass identifiera et signalera **faible** les mots de passe stockés dans votre coffre-fort sur la base d'un algorithme interne exécuté localement qui prend en compte divers critères tels que la longueur du mot de passe, la variété des caractères et l'inclusion de chiffres ou de lettres majuscules, entre autres facteurs.
- Anciens mots de passe : les mots de passe qui ont été enregistrés et non modifiés pendant plus de six mois seront signalés comme **vieux**.
- Mots de passe dupliqués : étant donné que l'utilisation des mêmes mots de passe sur plusieurs plateformes et comptes présente un risque de sécurité important, SecurePass signalera les mots de passe utilisés à plusieurs endroits comme **dupliquer**.

4.4. Organisation des données

Dans Bitdefender SecurePass, vous pouvez organiser et donc gérer plus facilement tous vos éléments enregistrés.

Vous pouvez classer vos articles dans des dossiers spécifiques pour y accéder facilement en suivant ces étapes :

1. Ouvrez Bitdefender SecurePass et accédez à **Mon coffre**. Ici, appuyez sur **Ajouter un dossier** bouton.
2. Donnez un nom à votre dossier et appuyez sur **Créez** bouton.
   Le nouveau dossier apparaîtra désormais dans votre coffre-fort.

Pour déplacer des éléments vers le dossier que vous avez créé :

1. Cliquez sur le compte que vous souhaitez déplacer et appuyez sur **Modifier** bouton.
2. Appuyez sur l'emplacement indiqué à côté de **Enregistrer l'article dans** et sélectionnez le nom du dossier dans la liste déroulante.
3. Appuyez sur **Enregistrer le compte** bouton.

Le compte sera désormais stocké dans le dossier sélectionné.

4.5. Remplissage automatique intelligent

Bitdefender SecurePass vous permet de saisir automatiquement les informations d'identification et les informations de votre compte sur tous les formulaires de connexion en ligne.

> **Remarque**
> En tant qu'extension de navigateur Web, sous Windows ou macOS, la fonction de remplissage automatique devrait fonctionner parfaitement.

4.5.1. Remplissage automatique sur Android

Pour configurer SecurePass sur Android afin d'utiliser la saisie automatique :

1. Ouvrez l'application Bitdefender SecurePass sur votre appareil Android.
2. Appuyez sur **Plus** bouton de menu.
3. En haut de l'écran, appuyez sur **Réglages**.
4. Tapez sur **Faites-en votre gestionnaire de mots de passe par défaut**
5. Activez Bitdefender SecurePass dans la liste des services de saisie automatique.

> **Remarque**
> Vous pouvez également accéder aux paramètres de votre appareil Android, dans **Mots de passe et comptes** > **Service de remplissage automatique** > activez Bitdefender SecurePass.
>
> Pour Android 11 ou les versions antérieures du système d'exploitation, les paramètres sont les suivants : **Système** > **Langue et saisie** > **Avancé**.

6. Tapotez **OK**.

Une fois cette configuration terminée, chaque fois que vous appuyez sur un champ de connexion, une option appelée Bitdefender SecurePass apparaît sur votre écran. Vous pouvez appuyer dessus pour ouvrir l'application. Connectez-vous à SecurePass et vos informations d'identification seront automatiquement renseignées

4.5.2. Remplissage automatique sur iOS

Pour configurer SecurePass sur votre appareil iOS afin d'utiliser la saisie automatique :

1. Ouvrez le **Réglage** application sur votre iPhone ou iPad, puis sélectionnez **Général**.
2. Tapez sur **Remplissage automatique et mots de passe**. Assurez-vous de l'option **Remplissage automatique des mots de passe et des clés d'accès** ou **Remplissage automatique des mots de passe** - selon la version iOS - est activée.
3. Dans le **Formulaire de remplissage automatique** liste, activez le **Bitdefender SecurePass** candidature.

Une fois cette configuration terminée, chaque fois que vous appuyez sur un champ de connexion, une option appelée Bitdefender SecurePass apparaît sur votre écran. Vous pouvez appuyer dessus pour ouvrir l'application. Connectez-vous à SecurePass et vos informations d'identification seront automatiquement renseignées

4.5.3. Informations sur la carte à remplissage automatique

Alors que SecurePass propose une icône facilement accessible permettant de remplir automatiquement les informations de connexion et les mots de passe, la fonction de saisie automatique des informations de carte de crédit fonctionne différemment :

1. Accédez à la page de paiement ou de paiement du site Web sur lequel vous souhaitez utiliser les informations de votre carte de crédit stockées.
2. Cliquez avec le bouton droit de la souris sur une zone vide de la page de paiement. Cela fera apparaître le menu contextuel sur votre écran.
3. Sélectionnez Bitdefender SecurePass dans le menu en plaçant votre curseur sur l'option. Cela ouvrira un sous-menu contenant d'autres options
4. Choisissez le **Saisie automatique des informations de carte de crédit**. Cela affichera la liste de toutes les cartes de crédit que vous avez stockées dans le coffre-fort SecurePass
5. Sélectionnez la carte préférée.

De cette façon, SecurePass remplira automatiquement les champs du formulaire de paiement avec les informations de la carte de crédit que vous avez choisie.

5. UTILISATION EN TANT QU'APPLICATION 2FA

Vous pouvez toujours choisir d'utiliser Bitdefender SecurePass comme application d'authentification à deux facteurs pour le site Web ou la plateforme de votre choix, et gérer vos codes 2FA ainsi que vos mots de passe de la manière suivante :

1. Accédez aux paramètres de sécurité du site Web ou de l'application sur lequel vous souhaitez activer la fonction 2FA. En règle générale, un code QR ou un code de vérification vous sera présenté au cours du processus.
2. Lancez Bitdefender SecurePass et accédez au compte correspondant que vous souhaitez configurer pour l'utilisation de l'authentification à deux facteurs. Cliquez sur **Modifier** bouton.
3. Faites défiler la page de création de compte dans SecurePass vers le bas et appuyez sur **Authentification à deux facteurs** option.
4. Scannez le code QR ou saisissez-le manuellement.
   Une fois cela fait, SecurePass confirmera la réussite de la configuration de l'authentification à deux facteurs.
5. Ensuite, appuyez sur le nouveau **Afficher le code** bouton désormais visible dans l'interface. Un code sensible au facteur temps y est affiché
6. Revenez sur le compte sur lequel vous avez activé la fonctionnalité 2FA et saisissez le code de Bitdefender SecurePass pour vérifier votre configuration.

Une fois ce processus de configuration terminé, appuyez sur **Enregistrer le compte** bouton dans SecurePass pour finaliser le processus.

Désormais, lorsque vous vous connectez sur la plateforme pour laquelle vous avez configuré la fonction 2FA, vous serez invité à utiliser les codes 2FA de SecurePass pour le compte concerné, offrant ainsi un nouveau niveau de sécurité pour le compte en question.

6. PARTAGE DE DONNÉES

Bitdefender SecurePass offre la possibilité de partager des informations sensibles en toute sécurité, telles que des informations d'identification, des mots de passe ou des informations de carte de crédit.

Vous pouvez utiliser la fonction de partage via les liens suivants :

1. Choisissez un objet stocké dans votre coffre-fort.
   - Dans le navigateur :
     Accédez à votre coffre-fort et cliquez sur l'objet que vous souhaitez partager. Sur le côté droit, cliquez sur le menu à trois points et sélectionnez **Partager le lien**.
   - Dans l'application :
     Accédez à votre coffre-fort et appuyez sur l'élément que vous souhaitez partager. Appuyez sur l'icône du lien et choisissez **Générer un lien de partage** option.
2. Créez le lien Partager en spécifiant :
   - Date d'expiration du lien.
   - La limite d'utilisation.
   - Si le lien doit être protégé par mot de passe ou non.
3. Une fois généré, copiez le lien généré et envoyez-le au destinataire.

6.1. Partagez avec des groupes

Les groupes sont créés dans le but de faciliter encore plus le partage de données. Vous pouvez créer différents groupes au sein de Bitdefender SecurePass avec d'autres utilisateurs afin de partager des données sensibles en toute sécurité

1. Créez un groupe :
   - Accédez à **Groupes** et appuyez sur **Créer un groupe** bouton dans l'onglet Groupes.
   - Définissez un nom de groupe, puis appuyez sur **Créer un groupe** bouton.

2. Ajouter des articles aux groupes :
   - Dans le navigateur :
     Accédez à votre coffre-fort et cliquez sur l'objet que vous souhaitez partager. Cliquez sur le menu à trois points sur le côté droit de l'élément et choisissez **Ajouter au groupe**.
   - Dans l'application :
     Accédez à votre coffre-fort et cliquez sur l'objet que vous souhaitez partager. Choisissez le **Partagez avec le groupe** option.

   Sélectionnez le groupe avec lequel vous souhaitez partager l'article.
3. Définissez les droits d'accès (lecture, écriture, octroi) en fonction du niveau de contrôle que vous souhaitez accorder aux membres du groupe.
4. Presse **Enregistrer**, puis **Terminé**.

Vous et les membres du groupe pouvez consulter les éléments partagés dans la section du groupe.

6.2. Gérer les groupes

Dans le **Groupes** section de Bitdefender SecurePass, vous pouvez consulter tous les groupes créés et les gérer en fonction de vos besoins :

- Renommez les groupes.
- Modifiez les membres. (inviter de nouveaux membres, attribuer des droits à des membres spécifiques, accorder des droits d'administrateur ou de partage, et supprimer des membres existants)
- Quittez les groupes.
- Supprimez des groupes.

7. VERROUILLER LE COMPTE

Bitdefender SecurePass est livré avec **Verrouiller le compte** fonction qui verrouille instantanément votre compte et met fin à toutes les sessions actives sur tous les appareils qui y ont accès. Cette fonctionnalité est particulièrement utile en cas de suspicion d'accès non autorisé.

Pour verrouiller votre compte SecurePass :

1. Ouvrez Bitdefender SecurePass.
2. Une fois dans SecurePass :
   - Dans le navigateur :
     Cliquez sur **Réglages** dans le coin supérieur droit de la page.
   - Dans l'application mobile :
     Appuyez sur **Sécurisez-moi** bouton de menu.
3. Appuyez sur **Verrouiller le compte** bouton pour vous déconnecter instantanément de tous les appareils et mettre fin aux sessions en cours.

8. 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

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).

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.

Qu'est-ce que le mode hors ligne ?

Le mode hors ligne est automatiquement activé lorsque la connexion Internet est interrompue lors de l'utilisation de Bitdefender SecurePass. Si vous êtes déjà connecté et que vous avez saisi 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 :

- 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.

9. OBTENIR DE L'AIDE

9.1. 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.

9.2. 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.

9.2.1. 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 donnés 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/.

9.2.2. 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/

9.2.3. 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.

9.3. 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/

9.3.1. 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 essayent 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 essayent 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 trousses administrateur ne sont pas nécessairement malveillants. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des trousses 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 trousses 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 partagiciels et logiciels gratuits pouvant être téléchargés sur Internet. Notons toutefois que la plupart des partagiciels et 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 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 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.

Réseau privé virtuel (VPN)

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.