Bitdefender®

PASSWORD MANAGER

BENUTZERHANDBUCH

Bitdefender Password Manager

Bedienungsanleitung

Veröffentlichungsdatum: 21.11.2022

Impressum

Bitdefender

Inhaltsverzeichnis

ÜBER DIESEN LEITFADEN

Zielsetzung und Zielgruppe

Dieses Handbuch richtet sich an alle Bitdefender-Benutzer auf allen unterstützten Betriebssystemen (Windows, MacOS, Android, iOS), die sich dafür entschieden haben Bitdefender Password Manager als ihr bevorzugtes Tool zur Passwortverwaltung. Die in diesem Buch präsentierten Informationen sind nicht nur für Computerkundige geeignet, sondern dienen auch als zugänglicher und freundlicher Leitfaden für jedermann.

Wir stellen Ihnen alle Funktionen und Merkmale im Detail vor, um Ihnen eine optimale Nutzung unseres ultrasicheren und funktionsreichen Passwortmanagers zu ermöglichen.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

Über dieses Handbuch

Dieses Handbuch behandelt die folgenden Themengebiete:

Einstieg (Seite 6)

Beginnen Sie mit Bitdefender Password Manager und den Installationsprozess.

Eigenschaften & Funktionalitäten (Seite 21)

Erfahren Sie, wie Sie es verwenden Bitdefender Password Manager und all seine Funktionen.

Hilfe bekommen (Seite 33)

Hinweise zu nützlichen Informationen und Hilfestellungen bei unerwarteten Problemen.

Konventionen in diesem Handbuch

Typografie

Zur Verbesserung der Lesbarkeit werden in diesem Handbuch verschiedene Textformate verwendet. Die Bedeutung der verschiedenen Formate können Sie der untenstehenden Tabelle entnehmen.

Erscheinungsbild	Beschreibung
`sample syntax`	Syntaxbeispiele sind mit gedruckt `monospaced` Figuren.
https://www.bitdefender.com	Verweise (Links) auf externe Inhalte auf HTTP- oder FTP-Servern.
documentation@bitdefender.com	Verweise auf E-Mail-Adressen, z. B. zur Kontaktaufnahme.
Über diesen Leitfaden (Seite 1)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
`filename`	Dateien und Verzeichnisse werden mit gedruckt `monospaced` Schriftart.
Möglichkeit	Alle Produktoptionen werden mit gedruckt **deutlich** Figuren.
Stichwort	Wichtige Schlüsselwörter oder Phrasen werden mit hervorgehoben **deutlich** Figuren.

Zusätzliche Hinweise

Zusätzliche Hinweise sind im Text grafisch markiert und liefern ergänzende Informationen zum aktuellen Absatz, die Sie unbedingt beachten sollten.

Notiz

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.

Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.

Warnung

Diese kritische Information sollten Sie mit höchster Aufmerksamkeit verfolgen. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst prekäre Thematik handelt.

Ihre Mithilfe

Wir laden Sie dazu ein uns bei der Verbesserung dieses Dokuments mitzuhelfen. Wir haben sämtliche Informationen in diesem Dokument bestmöglich überprüft um somit die Qualität sicherzustellen.

Lassen Sie es uns wissen, indem Sie eine E-Mail an senden documentation@bitdefender.com. Schreiben Sie alle Ihre

dokumentationsbezogenen E-Mails auf Englisch, damit wir sie effizient bearbeiten können.

1. WAS IST BITDEFENDER PASSWORD MANAGER

Bitdefender Password Manager ist ein plattformübergreifender Dienst, der Benutzern helfen soll, alle ihre Online-Passwörter zu speichern und zu organisieren. Es wurde mit den stärksten bekannten kryptografischen Algorithmen für ein Höchstmaß an Sicherheit und digitaler Sicherheit entwickelt. Es funktioniert als Browsererweiterung und mobile App-Lösung für Identitäts- und Passwortverwaltung, Bankgeschäfte und alle anderen Arten von sensiblen Informationen auf allen Geräten.

Bitdefender Password Manager kann Ihre Passwörter für alle Websites und Online-Dienste mit Hilfe eines einzigen Master-Passworts automatisch speichern, automatisch ausfüllen, generieren und verwalten, wodurch Ihre gesamte digitale Identität viel einfacher zu verwalten ist.

1.1. Sicherheit und wie es funktioniert

Hinter Bitdefender Password Manager Die Software verfügt über einige der neuesten kryptografischen Algorithmen, die die höchste Datensicherheit gewährleisten, auf die Benutzer hoffen können, wie AES-256-CCM-, SH512-, BCRYPT-, HTTPS- und WSS-Protokolle für die Datenübertragung. Alle beteiligten Daten werden zu jedem Zeitpunkt lokal ver- und entschlüsselt. Dies macht es so, dass nur der Kontoinhaber allein Zugriff auf die im Konto gespeicherten Informationen sowie auf das Master-Passwort haben kann, das für den Zugriff und die anschließende Nutzung der betreffenden Daten verwendet wird.

1.2. Password Manager Test- und kostenpflichtige Versionen

Die Testversion von Bitdefender Password Manager funktioniert mit allen Konten identisch mit der kostenpflichtigen Version des Produkts, aber ihre Verfügbarkeit läuft 90 Tage nach ihrer Aktivierung ab.

> **Notiz**
> Beachten Sie, dass die kostenpflichtige Version des Produkts zwar als reines Standalone-Produkt erworben werden kann, der unbegrenzte Zugriff auf den Passwort-Manager jedoch in den Abonnements „Bitdefender Premium Security“ und „Bitdefender Ultimate Security“ enthalten ist.

1.3. Bitdefender-Wallet- und Passwort-Manager

Viele Benutzer, die unsere Bitdefender-Wallet-Funktion in der Vergangenheit kennengelernt oder verwendet haben, fühlen sich vom „Passwort-Manager“ angezogen, weil sie eine aktualisierte Version der bereits vorhandenen Systeme sehen, die wir installiert haben. Wir denken, dass es sehr wichtig ist, die Unterscheidung zwischen diesen Produkten klar zu machen.

Bitdefender Wallet und Bitdefender Password Manager sind nicht dasselbe Produkt, der Hauptunterschied besteht in der plattformübergreifenden Passwortsynchronisierung. Password Manager ist eine eigenständige Software, die mit Windows-, Android-, macOS- und iOS-Geräten kompatibel ist, während Wallet ein Passwort-Manager-Modul mit grundlegenden Funktionen ist, das in unseren kostenpflichtigen Sicherheitslösungen (Bitdefender Antivirus Plus, Bitdefender Internet Security, Bitdefender Total Security) enthalten ist. Das Wallet ist nur unter Windows verfügbar und mit allen anderen Betriebssystemen nicht kompatibel.

- Wallet lässt sich nur mit den folgenden Browsern integrieren: Chrome, Firefox, Internet Explorer und Bitdefender Safepay.
- Im Gegensatz zu Password Manager bietet Wallet dem Benutzer keine Option zur Wiederherstellung des Master-Passworts. Das bedeutet, dass der Verlust Ihres Master-Passworts den Verlust aller vom Wallet-Modul verwalteten Passwörter zur Folge hat.
- Wallet-Funktionen sind auf Autosave & AutoFill, Auto-Lock und Passwort-Generator beschränkt.
- Sie können Daten aus anderen Passwortverwaltungsanwendungen nur in Ihr Wallet importieren **.db** Und **.csv** Formate.

Wir werden die für Password Manager verfügbaren Funktionen und alle Verbesserungen und zusätzlichen Funktionen, die ihn von unserem integrierten Wallet-Modul unterscheiden, weiter untersuchen und ausführlich besprechen.

2. EINSTIEG

2.1. Systemanforderungen

Sie können die neueste Version von verwenden Bitdefender Password Manager nur auf Geräten mit folgenden Betriebssystemen:

- **Für PC-Benutzer:**
  - Windows 7 mit Service Pack 1
  - Windows 8
  - Windows 8.1
  - Windows 10
  - Windows 11
- **Für macOS-Benutzer:**
  - macOS 10.14 (Mojave) und neuere macOS-Betriebssysteme

  Notiz
  Bitte beachten Sie, dass die Systemleistung auf Geräten mit Prozessoren älterer Generationen beeinträchtigt sein kann.
- **Für iOS-Benutzer:**
  - iOS 11.0 oder neuere iOS-Betriebssysteme
- **Für Android-Benutzer:**
  - Android 5.1 und neuere Android-Betriebssysteme

  Notiz
  - Die Funktion zum Entsperren per Fingerabdruck wird unterstützt **Android 6.0** und später.
  - Die Autofill-Funktion wird unterstützt **Android 8.0** und höher, kompatibel mit iPhone, iPad und iPod touch.

2.1.1. Software-Anforderungen

Verwenden zu können Bitdefender Password Manager und all seinen Funktionen müssen Ihre Windows- oder macOS-Geräte die folgenden Softwareanforderungen erfüllen:

- **Microsoft Edge** (basierend auf Chromium 80 und höher)
- **Mozilla-Firefox** (ab Version 65)
- **Google Chrome** (ab Version 72)
- **Safari** (ab Version 12)

Notiz
Die Softwareanforderungen gelten nicht für Android und iOS.

Warnung
Die Nichterfüllung der oben aufgeführten Systemanforderungen führt dazu, dass die Installation nicht möglich ist Bitdefender Password Manager oder die Fehlfunktion des Produkts.

2.2. Installation

Dieses Kapitel führt Sie durch die Installation Bitdefender Password Manager sowohl auf die Webbrowser auf Ihrem Windows-PC und macOS als auch auf Ihren mobilen Android- oder iOS-Geräten.

Wichtig
Stellen Sie vor der Installation sicher, dass Sie über ein gültiges Password Manager-Abonnement verfügen Bitdefender-Zentrale Konto, damit diese Browsererweiterung ihre Gültigkeit von Ihrem Konto abrufen kann.

Aktive Abonnements sind in der aufgeführt **Meine Abonnements** Abschnitt in Bitdefender Central.

2.2.1. Installation auf Windows- und macOS-Geräten

Anders als die meisten Desktop-Anwendungen und Softwarelösungen, die auf diesen Geräten installiert und eingerichtet werden müssen, wird der Bitdefender Password Manager als Browsererweiterung - auch Add-on genannt - bereitgestellt, die im Handumdrehen zu Ihrem bevorzugten Browser hinzugefügt und aktiviert werden kann.

Die derzeit unterstützten Browser für das Produkt sind die folgenden: **Google Chrome**e, **Mozilla-Firefox**, **Microsoft Edge**, Und **Safari**.

1. Gehe zu https://central.bitdefender.com/ und melden Sie sich bei Ihrem Konto an.
   Wenn Sie noch kein Konto haben, klicken Sie auf **BENUTZERKONTO ERSTELLEN**, geben Sie dann Ihren vollständigen Namen, eine E-Mail-Adresse und ein Passwort ein.
2. Wählen **Meine Geräte** in der linken Seitenleiste des Bildschirms.
3. Im **Meine Geräte** Abschnitt, fahren Sie fort, indem Sie auf klicken **+ Gerät hinzufügen**.
4. Diese Aktion wird dazu führen, dass ein neues Fenster erscheint. Wählen **Passwortmanager** im Selektionsbild.
5. Wählen **Dieses Gerät**.
   Wenn Sie die Installation auf einem anderen Gerät vornehmen möchten, klicken Sie auf Weitere Geräte. Sie können dann einen Download-Link per E-Mail an das jeweilige Gerät senden oder die URL für die Installation selbst kopieren.
6. Wählen Sie anschließend den Browser aus, für den Sie die Password Manager-Erweiterung installieren möchten.
7. Über die entsprechende Schaltfläche gelangen Sie direkt zum Erweiterungsangebot des Browsers. Folgen Sie dort einfach den Anweisungen auf dem Bildschirm, wie im Folgenden gezeigt:

   Microsoft Edge

   - Drücke den **Erhalten** Taste
   - Klicken **Erweiterung hinzufügen** in der Eingabeaufforderung, die auf dem Bildschirm erscheint

   Google Chrome

   - Drücke den **Zu Chrome hinzufügen** Taste
   - Klicken Sie im Bestätigungsfeld auf **Erweiterung hinzufügen**

   Mozilla-Firefox

   - Drücke den **Zu Firefox hinzufügen** Taste
   - Drücke den **Installieren** Schaltfläche in der oberen rechten Ecke des Bildschirms

Safari

- Drücke den **Erhalten** Taste, dann klicken **Installieren**
- Safari öffnen und auswählen **Einstellungen** in der oberen Menüleiste
- Klicken Sie im Fenster „Einstellungen“ auf die **Erweiterungen** Tab
- Markieren Sie das Kontrollkästchen neben dem Password Manager, um ihn zu aktivieren.

Nachdem Sie diese Schritte befolgt haben, legen Sie ein starkes Master-Passwort fest und drücken Sie dann die **Master-Passwort speichern** Schaltfläche, nachdem Sie gelesen haben und damit einverstanden sind **Geschäftsbedingungen**.

Wichtig

Bitte beachten Sie, dass Sie dieses Master-Passwort benötigen, um auf die im Bitdefender Password Manager gespeicherten Passwörter, Kreditkarteninformationen und Notizen zuzugreifen. Das Master-Passwort dient als Schlüssel, der eine Nutzung des Produkts erst möglich macht.

Warnung

Beim Erstellen des Master-Passworts erhalten Sie eine **24-stelliger Wiederherstellungsschlüssel**. Notieren Sie sich Ihren Wiederherstellungsschlüssel an einem sicheren Ort und verlieren Sie ihn nicht. Dieser Schlüssel ist die einzige Möglichkeit, auf Ihre in Password Manager gespeicherten Passwörter zuzugreifen, falls dies doch passieren sollte **vergessen Sie das Master-Passwort** zuvor für Ihr Konto eingerichtet.

- Sie können drücken **Schließen** wenn fertig.

2.2.2. Installation auf Android-Geräten

Der Bitdefender Password Manager lässt sich auf Android-Telefonen und -Tablets am einfachsten installieren, indem Sie die App direkt von Google Play herunterladen.

Die Installation der Bitdefender Password Manager-App kann auch über Ihren erfolgen Bitdefender-Zentrale Konto:

1. Melden Sie sich auf Ihrem Android-Mobilgerät bei Ihrem Bitdefender Central-Konto an, indem Sie darauf zugreifen https://login.bitdefender.com/central/login.
2. Wählen **Meine Geräte** in der linken Seitenleiste des Bildschirms.
3. Im **Meine Geräte** Abschnitt, fahren Sie fort, indem Sie auf klicken **+ Gerät hinzufügen**.
4. Diese Aktion wird dazu führen, dass ein neues Fenster erscheint. Wählen **Passwortmanager** im Selektionsbild.
5. Wählen **Dieses Gerät**.
   Wenn Sie auf einem anderen Gerät installieren möchten, wählen Sie **Andere Geräte**. Sie können dann einen Download-Link per E-Mail an das jeweilige Gerät senden oder die URL für die Installation direkt kopieren.
6. Sie werden weitergeleitet Google Play. Klopfen **Installieren** um Bitdefender Password Manager auf Android herunterzuladen.
7. Sobald der Download abgeschlossen ist, öffnen Sie die Password Manager-Anwendung.
8. Wenn Sie nicht automatisch bei Ihrem Konto angemeldet werden, melden Sie sich mit Ihrem Benutzernamen und Passwort an.
   Nachdem Sie diese Schritte befolgt haben, legen Sie ein starkes Master-Passwort fest und drücken Sie dann die **Master-Passwort speichern** Schaltfläche, nachdem Sie gelesen haben und damit einverstanden sind **Geschäftsbedingungen**.

> **Wichtig**
> Beachten Sie, dass Sie dieses Master-Passwort benötigen, um alle im Bitdefender Password Manager gespeicherten Passwörter, Kreditkarteninformationen und Notizen freizuschalten. Dies ist im Wesentlichen der Schlüssel, der es dem Besitzer ermöglicht, dieses Produkt zu verwenden.

Warnung

Beim Erstellen des Master-Passworts erhalten Sie eine **24-stelliger Wiederherstellungsschlüssel**. Notieren Sie sich Ihren Wiederherstellungsschlüssel an einem sicheren Ort und verlieren Sie ihn nicht. Dieser Schlüssel ist die einzige Möglichkeit, auf Ihre in Password Manager gespeicherten Passwörter zuzugreifen, falls dies doch passieren sollte **vergessen Sie das Master-Passwort** zuvor für Ihr Konto eingerichtet.

- Sie können drücken **Schließen** wenn fertig.

9. Ein ... kreieren **4-stellige PIN**, wenn Sie also zu einer anderen App wechseln und dann zu Password Manager zurückkehren, müssen Sie das zuvor eingerichtete Master-Passwort nicht erneut eingeben. Falls verfügbar, können Sie auch die Gesichtserkennung oder die Authentifizierung per Fingerabdruck aktivieren.
10. Tippen Sie auf **Automatisches Ausfüllen aktivieren** , um die Einstellungen für das automatische Ausfüllen von Android zu konfigurieren.

Notiz

Wenn Sie diesen Schritt überspringen, können Sie die AutoFill-Funktionen von Android zu einem späteren Zeitpunkt aktivieren und anpassen, indem Sie die Anweisungen unter befolgen Intelligentes automatisches Ausfüllen (Seite 22).

11. Es wird eine Liste mit Anwendungen angezeigt, die Passwörter automatisch ausfüllen können.
    Wählen **Passwortmanager** und dann fordert das Gerät Sie auf, zu bestätigen, dass Sie dieser App vertrauen.
    Klopfen **OK**.
12. Geben Sie die PIN ein, die Sie eingerichtet haben **Schritt 9** um diese Aktion zu bestätigen.

Die Installation auf Ihrem Android-Gerät ist damit abgeschlossen.

2.2.3. Installation auf iOS-Geräten

Der Bitdefender Password Manager lässt sich auf iOS- und iPadOS-Geräten am einfachsten installieren, indem Sie die App direkt aus dem App Store herunterladen.

Die Installation der Bitdefender Password Manager-App kann auch über Ihren erfolgen Bitdefender-Zentrale Konto:

1. Melden Sie sich dazu auf Ihrem iPhone oder iPad bei Ihrem Bitdefender Central-Konto an, indem Sie {1}https://login.bitdefender.com/central/login{2} aufrufen.
2. Wählen **Meine Geräte** in der linken Seitenleiste des Bildschirms.
3. Im **Meine Geräte** Abschnitt, fahren Sie fort, indem Sie auf klicken **+ Gerät hinzufügen**.
4. Diese Aktion wird dazu führen, dass ein neues Fenster erscheint. Wählen **Passwortmanager** im Selektionsbild.
5. Wählen **Dieses Gerät**.
   Wenn Sie auf einem anderen Gerät installieren möchten, wählen Sie **Andere Geräte**. Sie können dann einen Download-Link per E-Mail an das jeweilige Gerät senden oder die URL für die Installation direkt kopieren.
6. Sie werden weitergeleitet **Appstore**. Tippen Sie auf das Wolkensymbol mit einem nach unten zeigenden Pfeil, um Bitdefender Password Manager for iOS herunterzuladen.
7. Einmal die Anwendung installiert ist, öffnen Sie sie und aktivieren Sie das kleine Kästchen auf dem Bildschirm. Wählen **Weitermachen** nachdem Sie gelesen haben und damit einverstanden sind **Abonnentenvereinbarung**.
8. Wenn Sie nicht automatisch bei Ihrem Konto angemeldet werden, melden Sie sich mit Ihrem Benutzernamen und Passwort an.
   Nachdem Sie diese Schritte befolgt haben, legen Sie ein starkes Master-Passwort fest und drücken Sie dann die **Master-Passwort speichern** Schaltfläche, nachdem Sie gelesen haben und damit einverstanden sind **Geschäftsbedingungen**.

Wichtig

Beachten Sie, dass Sie dieses Master-Passwort benötigen, um alle im Bitdefender Password Manager gespeicherten Passwörter, Kreditkarteninformationen und Notizen freizuschalten. Dies ist im Wesentlichen der Schlüssel, der es dem Besitzer ermöglicht, dieses Produkt zu verwenden.

Warnung

Beim Erstellen des Master-Passworts erhalten Sie eine **24-stelliger Wiederherstellungsschlüssel**. Notieren Sie sich Ihren Wiederherstellungsschlüssel an einem sicheren Ort und verlieren Sie ihn nicht. Dieser Schlüssel ist die einzige Möglichkeit, auf Ihre in Password Manager gespeicherten Passwörter zuzugreifen, falls dies doch passieren sollte **vergessen Sie das Master-Passwort** zuvor für Ihr Konto eingerichtet.

- Sie können drücken **Schließen** wenn fertig.

9. Ein ... kreieren **4-stellige PIN**, wenn Sie also zu einer anderen App wechseln und dann zu Password Manager zurückkehren, müssen Sie das zuvor eingerichtete Master-Passwort nicht erneut eingeben. Falls verfügbar, können Sie auch die Gesichtserkennung oder die Authentifizierung per Fingerabdruck aktivieren.

Die Installation auf Ihrem iOS/iPadOS-Gerät ist damit abgeschlossen.

3. IMPORTIEREN UND EXPORTIEREN IHRER PASSWÖRTER

Der Bitdefender Password Manager ist so aufgebaut, dass er die Kommunikation und Datenübertragung mit externen Quellen, Plattformen und Softwaretools effizient erleichtert. Dies ist der Hauptgrund, warum der sehr häufig auftretende Bedarf, Passwörter in oder aus Bitdefender Password Manager zu importieren oder zu exportieren, problemlos erfüllt werden kann.

3.1. Produktkompatibilität

Der Bitdefender Password Manager ermöglicht eine nahtlose Datenübertragung aus den folgenden Anwendungen:

- **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**

> **Notiz**
> Wenn der Name des Browsers oder Passwort-Manager-Tools, von dem Sie versuchen, Datendateien zu übertragen, nicht in der oben bereitgestellten Liste aufgeführt ist, können Sie unserer Online-Anleitung folgen, wie Benutzer eine CSV-Datei von nicht unterstützten Passwort-Managern bearbeiten können, damit Sie dies können Importieren Sie Ihre Informationen in **Bitdefender-Passwort-Manager**: https://www.bitdefender.com/consumer/support/answer/2472/

Dieser Datentransfer zwischen dem Bitdefender Password Manager und anderen Lösungen kann über die folgenden Datenformate erfolgen:

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

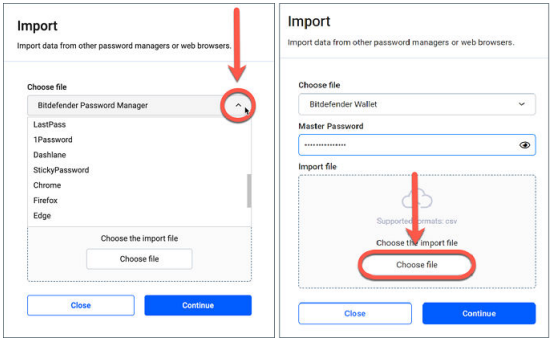
3.2. Import in den Password Manager

Der Bitdefender Password Manager ermöglicht Ihnen den einfachen Import von Passwörtern aus anderen Passwortmanagern und Browsern. Wenn Sie von einem anderen Passwortverwaltungsdienst zu Bitdefender Password Manager wechseln möchten, haben Sie dort vermutlich eine beträchtliche Menge an Anmeldedaten wie Benutzernamen, Passwörter und andere Login-Informationen für Ihre Konten gespeichert.

Mit dem Umstieg auf den Bitdefender Password Manager möchten Sie diese gespeicherten Daten bestimmt auch mitnehmen.

So importieren Sie Ihre gespeicherten Informationen aus anderen Apps und Webbrowsern in Bitdefender Password Manager, **unabhängig vom Betriebssystem** auf dem Sie dieses Produkt installieren möchten:

1. Klicken Sie in Ihrem Webbrowser (unter Windows oder macOS) auf das Password Manager-Symbol oder starten Sie die Password Manager-Anwendung (unter Android oder iOS). Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.
2. Öffnen Sie den Passwort-Manager Menü, um die Seitenleiste auf der linken Seite zu erweitern, und klicken Sie auf **Einstellungen** Menüpunkt.
3. Scrollen Sie nach unten zu **Daten** Abschnitt und klicken Sie auf die **Daten importieren** Möglichkeit.
4. Verwenden Sie das Dropdown-Menü, um den Namen der Passwort-Manager-App oder des Browsers auszuwählen, aus dem Sie Ihre Konten importieren möchten. Geben Sie Ihre ein Master Passwort in das entsprechende Feld ein und klicken Sie dann auf **Datei wählen**.



5. Durchsuchen Sie Ihre Ordner, um den Speicherort zu finden, an dem Sie die Datei mit Ihren Benutzernamen und Passwörtern gespeichert haben, die Sie von Ihrem anderen Passwort-Manager oder Webbrowser exportiert haben, und drücken Sie dann **Weitermachen**.

Nach dem Import sind Ihre Passwörter dann auf allen Geräten verfügbar, auf denen die Bitdefender Password Manager-App bzw. die Browsererweiterung installiert ist.

3.3. Export aus dem Password Manager

Mit dem Bitdefender Password Manager können Sie Ihre gespeicherten Passwörter (einschließlich Anmeldedaten, sichere Notizen usw.) ganz

einfach in eine CSV-Datei (Comma-separated values) oder verschlüsselte Datei exportieren. So möchten wir Ihnen den Umstieg so einfach wie möglich machen, sollten Sie vom vom Bitdefender Password Manager zu einem anderen Passwortmanager-Dienst wechseln möchten.

> **Wichtig**
> Eine CSV-Datei ist **nicht** verschlüsselt und enthält Benutzernamen und Passwörter im Klartextformat, was bedeutet, dass Ihre privaten Informationen von jedem gelesen werden können, der Zugriff auf Ihr Gerät hat. Wir empfehlen Ihnen daher, die nachstehenden Anweisungen auf einem vertrauenswürdigen Gerät zu befolgen.

So exportieren Sie Ihre Daten aus dem Bitdefender Password Manager:

1. Klicken Sie in Ihrem Webbrowser (unter Windows oder macOS) auf das Password Manager-Symbol oder starten Sie die Password Manager-Anwendung (unter Android oder iOS). Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.
2. Öffnen Sie das Password Manager-Menü, um die Seitenleiste auf der linken Seite zu erweitern, und klicken Sie auf **Einstellungen** Menüpunkt.
3. Scrollen Sie nach unten zu **Daten** Abschnitt und klicken Sie auf die **Daten exportieren** Möglichkeit.
4. Ihnen sollten nun die folgenden beiden Optionen angezeigt werden:
   - **CSV**
   - **Passwortgeschützte Dateien**

   Wählen Sie Ihre bevorzugte Option, geben Sie Ihr Master-Passwort ein und klicken Sie auf **Daten exportieren** Taste.

   > **Notiz**
   > Wenn Sie die Option "Passwortgeschützte Datei" wählen, werden Sie aufgefordert, die Daten mit der Liste Ihrer Konten mit einem Passwort zu verschlüsseln, so dass nur Sie bei Bedarf darauf zugreifen können.

5. Ihr Webbrowser/Ihre App fährt fort, indem sie eine Datei mit dem Namen speichert `Bitdefender Password Manager_exported_data_current-date` auf Ihr System im

Standard-Download-Ordner. Es enthält alle Ihre im Bitdefender Password Manager gespeicherten Daten.

Nach dem Export Ihrer Daten können Sie diese in einen Passwortmanager Ihrer Wahl hochladen.

3.4. Übertragen Ihrer Bitdefender-Geldbörse in den Password Manager

Weil viele unserer Benutzer, die sich für Bitdefender Password Manager als ihren Passwortverwaltungsdienst entschieden haben, zuvor unsere bereits vorhandene Funktion verwendet haben **Bitdefender-Wallet**, möchten wir zeigen, wie Sie die Daten innerhalb der Brieftasche verwenden und Ihre Kontoanmeldeinformationen in das neue und verbesserte Password Manager-Produkt übertragen sowie die beiden Dienste über die Cloud synchronisieren.

> **Notiz**
> Da Wallet eine Funktion ist, die nur auf Windows-Geräten verfügbar ist, sind diese Anweisungen nur für Windows-Betriebssysteme gedacht. Sie müssen die Wallet-Datenbank exportieren und in Password Manager importieren **nur einmal**.

1. **Gespeicherte Passwörter aus Wallet in eine CSV-Datei exportieren:**

   a. Nachdem Sie Ihr Bitdefender-Produkt auf die neueste Version aktualisiert und Windows neu gestartet haben, öffnen Sie die `C:\Program Files\Bitdefender\Bitdefender Security` Ordner auf Ihrem Computer, suchen Sie die Datei mit dem Namen und doppelklicken Sie darauf `bdwtxcon`.

   b. Klicken Sie anschließend auf die **Jetzt anfangen** Schaltfläche auf dem Willkommensbildschirm.

   c. Aktivieren Sie das Kontrollkästchen neben dem Namen des Wallets, das Sie exportieren möchten, und klicken Sie auf **Nächste** Taste. Wenn mehrere Wallets ausgewählt sind, werden alle ihre Passwörter in einer einzigen Datei zusammengeführt.

   d. Geben Sie Ihre ein Master Passwort Um die im vorherigen Schritt ausgewählte Brieftasche zu entsperren, drücken Sie dann die **Geldbörse hinzufügen** Taste.

   e. Sobald die Datenbank bereit ist, wird eine Zusammenfassung der aus dem Wallet exportierten Konten angezeigt. Drücke den **Speichern Sie Ihre Daten** Taste.

   f. Wenn Sie dazu aufgefordert werden, wählen Sie einen Namen für die CSV-Datei und speichern Sie sie an einem leicht auffindbaren

Ort – beispielsweise auf Ihrem Desktop. Bitdefender exportiert alle Ihre gespeicherten Anmeldedaten in diese Datei.

2. **Importieren der aus Wallet exportierten CSV-Datei in Password Manager:**
   a. Klicken Sie auf das Password Manager-Symbol in der Symbolleiste Ihres Webbrowsers. Geben Sie Ihr Master-Passwort ein, wenn Sie dazu aufgefordert werden.
   b. Öffnen Sie das Password Manager-Menü , um das Seitenleistenmenü auf der linken Seite zu erweitern, und klicken Sie auf **Einstellungen** Menüpunkt.
   c. Scrollen Sie nach unten zu **Daten** Abschnitt und klicken Sie auf die **Daten importieren** Möglichkeit.
   d. Wählen **Bitdefender-Wallet** Geben Sie aus der Liste der Passwort-Manager Ihre ein Master Passwort in das entsprechende Feld ein und klicken Sie dann auf **Datei wählen**.
   e. Wählen Sie die CSV-Datei mit Ihren Benutzernamen und Passwörtern aus, die aus dem Wallet exportiert wurden, und drücken Sie dann **Weitermachen**.

3. **Löschen der aus Wallet exportierten CSV-Datei:**
   a. Rufen Sie Ihre Bitdefender-Sicherheitslösung auf und gehen Sie zu **Privatsphäre** auf der linken Seite der Benutzeroberfläche.
   b. Im **Passwortmanager** Bereich anklicken **Einstellungen**.
   c. Klicken Sie auf die beschriftete Registerkarte **Meine Geldbörsen**.
   d. Am unteren Rand des Fensters sehen Sie eine Warnung, die Sie über unverschlüsselte Daten auf Ihrem Computer informiert. Klicke auf **Dateien schreddern**.
   e. Drücken Sie im File Shredder-Bildschirm **Dauerhaft löschen** und bestätigen Sie die Aktion.

4. EIGENSCHAFTEN & FUNKTIONALITÄTEN

Dieses Kapitel führt Sie durch alle Features und Funktionen des Bitdefender Password Managers und erklärt deren Nützlichkeit und wie Sie sie am effizientesten bedienen.

4.1. Richtiger Umgang mit Passwörtern

4.1.1. Passwortgenerator

Die wichtigste Regel für mehr Sicherheit im Internet ist die konsequente Nutzung von zufällig gewählten Passphrasen für jeden Dienst, für den ein Benutzerkonto erstellt werden muss. Dabei darf jede Passphrase immer nur einmal vergeben werden. Die Wiederverwendung von Passwörtern über mehrere Dienste hinweg ist die Hauptursache für Identitätsdiebstahl und andere Schäden im Zusammenhang mit der betrügerischen Übernahme von Konten.

Diese Funktion hilft Benutzern bei der Erstellung sicherer, komplexer und einzigartiger Passwörter für jedes neue Online-Benutzerkonto. Sie müssen nie sich nie wieder selbst sichere Passwörter ausdenken und merken oder darauf achten, das gleiche Passwort nicht mehrfach zu vergeben.

Der **Passwortgenerator** kann über die Registerkarte oben auf der Benutzeroberfläche von Password Manager aufgerufen werden.

Der Generator kann so eingestellt werden, dass er Passwörter zurückgibt **zwischen 4 und 32 Zeichen**.

Sie können auch die Arten von Zeichen angeben, die im zufällig generierten Passwort vorhanden sein sollen oder nicht, indem Sie die entsprechenden Kontrollkästchen aktivieren oder deaktivieren. **(Kleinbuchstaben, Großbuchstaben, Zahlen, Sonderzeichen)**

Durch Drücken der ↻ rechts neben dem angezeigten Passwort, ändert der Generator das vorgeschlagene Passwort.

Um das angezeigte Passwort zu verwenden, drücken Sie **Passwort verwenden**, Aktion, die die Zeichenfolge in Ihrer Zwischenablage speichert.

> **Notiz**
> Ihre zuvor generierten Passwörter werden vorübergehend im Passwortverlauf gespeichert, auf den Sie über zugreifen können **Passwortverlauf** Taste.

4.1.2. Passworterfassung

Mit dieser Funktion im Password Manager werden Sie aufgefordert, alle neuen Passwörter sofort nach der Erstellung zu speichern. Der Password Manager fordert Benutzer auf, ihre neu erstellten Passwörter zu speichern, damit sie sofort der von Bitdefender bereitgestellten ultrasicheren Umgebung hinzugefügt werden können.

4.1.3. Intelligentes automatisches Ausfüllen

Der Bitdefender Password Manager kann so eingerichtet werden, dass er Ihre Anmeldedaten und vor allem Ihre Passwörter automatisch ausfüllt. Von uns entwickelte Algorithmen erkennen bereits besuchte Websites und füllen Ihre Anmeldedaten für Sie aus, so dass Sie bei jeder Anmeldung bei Ihren Diensten Zeit sparen.

1. Klicken Sie unter Windows oder macOS auf die **Passwortmanager** Symbol in Ihrem Webbrowser.
   Starten Sie unter Android oder iOS die **Passwortmanager** Anwendung.
   Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.
2. Öffnen Sie das Password Manager-Menü , um die Seitenleiste auf der linken Seite zu erweitern, und klicken Sie auf **Einstellungen** Menüpunkt.
3. Klicke auf **Geräteeinstellungen**.
4. Hier sehen Sie eine Schaltfläche, die beides anzeigt **Deaktivieren Sie das automatische Ausfüllen** oder **Automatisches Ausfüllen aktivieren**. Diese Einstellung steuert den Betriebszustand der intelligenten Autofill-Funktion.

4.1.4. Sicherheitsbericht

Der Sicherheitsbericht ist ein Tool, das Berichte auf Grundlage verschiedener Funktionen erstellt, die Ihrer digitalen Sicherheit dienen.

So werden Sie nach Bewertung der Sicherheit vorhandener Passwörter zum Beispiel informiert, ob ein Passwort Ihre sofortige Aufmerksamkeit erfordert. Auch doppelte Passwörter werden erkannt. Sie werden dann aufgefordert, diese Passwörter entsprechend zu ändern, um die mit der Mehrfachnutzung verbundenen Risiken zu vermeiden.

Der Bericht liefert Ihnen hauptsächlich Informationen zu Ihren Passwortgewohnheiten, d. h. zu mehrfach genutzten Passwörtern, schwachen oder anderweitig kompromittierten Passwärtern und E-Mail-Adressen.

Dazu wird die Liste der verschlüsselten Hashes von Troys Website lokal auf Ihrem Gerät verglichen, um zu prüfen, ob sie die entsprechenden Hashes Ihrer Passwörter enthält. Wenn eine Übereinstimmung gefunden wird, werden Sie benachrichtigt, damit Sie Ihre Passwörter und andere Anmeldedaten ändern können.

Für den Zugriff auf die **Sicherheitsbericht**, rufen Sie die Password Manager-Oberfläche auf und wählen Sie die entsprechende aus Schaltfläche in der oberen Leiste.

4.1.5. Plattformübergreifende Synchronisierung

Wenn Sie Ihre Passwörter einmal im Bitdefender Password Manager gespeichert haben, können Sie diese auch auf all Ihren Windows-, Mac-, Android- oder iOS-Geräten in Chrome, Safari, Firefox und Edge oder in den mobilen Apps speichern und jederzeit sicher darauf zugreifen.

> **Notiz**
> Bitdefender ist auch mit einem ausgestattet **Offline-Modus** um auf Ihre Passwörter zuzugreifen, falls Sie keinen Zugang zum Internet haben. So sind Ihre Passwörter jederzeit und von überall zugänglich.

4.1.6. Löschen von Einträgen

Um gespeicherte Passwörter zu löschen, drücken Sie zuerst die Bearbeiten-Symbol neben dem Eintrag, den Sie entfernen möchten, befindet sich im **Konten** Tab. Scrollen Sie nach unten und wählen Sie dann aus **Löschen**. Wenn Sie gefragt werden, ob Sie das Konto wirklich entfernen möchten, wählen Sie aus **Entfernen**.

4.2. Richtiger Umgang mit Konten

4.2.1. Authentifizierung

Die Authentifizierung beim Bitdefender Password Manager erfolgt über die **STIFT** im Installationsprozess des Produkts eingerichtet. (Notiere dass der **Automatische Sperre** Funktion sperrt den Passwortmanager oder loggt sich nach einer gewissen Zeit der Inaktivität auf Browserebene oder Schließen der mobilen App aus)

Darüber hinaus kann dies auch durch die Verwendung von Biometrie erfolgen, sofern verfügbar, wie z **Fingerabdruck** oder **Gesichts Entsperrung**.

Zu **aktivieren oder deaktivieren** biometriebasierte Authentifizierung:

1. Klicken Sie unter Windows oder macOS auf die **Passwortmanager** Symbol in Ihrem Webbrowser.
   Starten Sie unter Android oder iOS die **Passwortmanager** Anwendung.
   Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.
2. Öffnen Sie das Password Manager-Menü , um die Seitenleiste auf der linken Seite zu erweitern, und klicken Sie auf **Einstellungen** Menüpunkt.
3. Klicke auf **Geräteeinstellungen**.
4. Hier sehen Sie eine Schaltfläche, die beides anzeigt **Biometrie deaktivieren** oder **Biometrie aktivieren**. Diese Einstellung steuert den Betriebszustand der biometriebasierten Authentifizierungsfunktion.

4.2.2. Zurücksetzen des Master-Passworts

> **Wichtig**
> Der **Master-Passwort ändern** Die Funktion ist auf Mobilgeräten nicht verfügbar. Sie können Ihr Master-Passwort nur über die Browsererweiterung Bitdefender Password Manager auf einem Windows-PC oder einem macOS-Gerät ändern oder wiederherstellen.

So ändern Sie Ihre Master Passwort als Vorsichtsmaßnahme und erstellen Sie ein neues im Bitdefender Password Manager.

1. Sobald Sie die Browsererweiterung installiert haben, klicken Sie auf die **Passwortmanager** Symbol in der Symbolleiste Ihres Webbrowsers.
2. Geben Sie Ihr aktuelles Master-Passwort ein, um den Tresor zu entsperren.

   Wichtig
   Wenn Sie sich nicht an das aktuelle Master-Passwort erinnern, klicken Sie auf **Ich habe mein Passwort vergessen** Option auf demselben Bildschirm. Geben Sie die ein **24-stelliger Wiederherstellungsschlüssel** das Sie während der Ersteinrichtung von Bitdefender Password Manager erhalten haben, und geben Sie dann ein neues Master-Passwort ein. **Wenn Sie es vergessen oder verlegen** beide Master Passwort und das **Wiederherstellungs-Schlüssel**, als letzten Ausweg, **Wenden Sie sich an einen Bitdefender-Vertreter, um Ihnen beim Zurücksetzen Ihres Kontos zu helfen**. Das Zurücksetzen Ihres Kontos wird Löschen Sie alle Ihre Daten und Passwörter im Bitdefender Password Manager gespeichert.

3. Öffnen Sie das Password Manager-Menü , um die Seitenleiste auf der linken Seite zu erweitern, und klicken Sie auf **Einstellungen** Menüpunkt.
4. Klick auf das **Mein Konto** Schaltfläche in der **Konto** Abschnitt.
5. Ein Fenster mit Informationen zu Ihrem Password Manager-Abonnement wird angezeigt.
   Klick auf das **Master-Passwort ändern** Taste.
6. Sie werden zu einem neuen Fenster weitergeleitet, in dem Sie ein neues Master-Passwort festlegen können. Geben Sie zunächst Ihr aktuelles Master-Kennwort und danach das neue Master-Passwort ein. Das neue Master-Kennwort muss mindestens 8 Zeichen lang sein und mindestens einen Kleinbuchstaben, einen Großbuchstaben und eine Zahl enthalten.
7. Drücken Sie die **Ändern** Taste, wenn Sie fertig sind.
8. Warten Sie einen Moment, bis Bitdefender das alte Master-Passwort zurückgesetzt hat.
   Schließen Sie Ihren Webbrowser nicht!

9. Als nächstes erhalten Sie eine neue **24-stelliger Wiederherstellungsschlüssel**. Notieren Sie sich den Wiederherstellungsschlüssel an einem sicheren Ort und **verliere es nicht**. Dieser Schlüssel ist die einzige Möglichkeit, auf Ihre im Password Manager gespeicherten Passwörter zuzugreifen, falls Sie das Master-Passwort vergessen.
   Drücken Sie **Schließen** wenn du fertig bist.
10. Sie werden von Bitdefender Password Manager abgemeldet.
    Geben Sie zum Entsperren des Tresors das neue Master-Passwort ein, das Sie gerade festgelegt haben.

4.3. Weitere Funktionen

4.3.1. Verwaltung von Identitäten

Mit dieser Funktion können Benutzer mehrere Identitäten speichern und mit dem Password Manager ihre Daten in Webformularen automatisch ausfüllen. So wird Online-Shopping schnell, einfach und sicher.

Wie alles andere im Password Manager sind auch die sensiblen Daten, die zu diesen gespeicherten Identitäten gehören, verschlüsselt und nur auf dem Gerät des Benutzers abrufbar.

So können Sie im Password Manager eine Identität hinzufügen:

1. Klicken Sie unter Windows oder macOS auf die **Passwortmanager** Symbol in Ihrem Webbrowser.
   Starten Sie unter Android oder iOS die **Passwortmanager** Anwendung.
   Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.
2. Öffnen Sie das Password Manager-Menü , um die Seitenleiste auf der linken Seite zu erweitern, und klicken Sie auf **Identitäten** Menüpunkt.
3. Drücken Sie auf die **Identität hinzufügen** Knopf unten.
4. Vervollständigen Sie die Details, die Sie speichern möchten, und drücken Sie dann **Speichern**.

4.3.2. Verwalten von Kreditkarten

Mit dieser Funktion können Sie Ihre Kreditkartendaten speichern und automatisch eingeben, um einfacher, schneller und sicherer einzukaufen.

So können Sie im Password Manager eine Kreditkarte hinzufügen:

1. Klicken Sie unter Windows oder macOS auf die **Passwortmanager** Symbol in Ihrem Webbrowser.
   Starten Sie unter Android oder iOS die **Passwortmanager** Anwendung.
   Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.
2. Öffnen Sie das Password Manager-Menü , um die Seitenleiste auf der linken Seite zu erweitern, und klicken Sie auf **Kreditkarten** Menüpunkt.
3. Drücken Sie auf die **Identität hinzufügen** Knopf unten.
4. Vervollständigen Sie die Details, die Sie speichern möchten, und drücken Sie dann **Speichern**.

4.3.3. Meine Absicherung

Mit der Funktion Meine Absicherung können Sie sich jederzeit per Fernzugriff abmelden und Ihren Browserverlauf auf Ihrem Computer, Tablet oder Mobilgerät löschen. Wir empfehlen diese Funktion besonders dann, wenn Sie Ihr Gerät nicht alleine nutzen.

So finden und aktivieren Sie diese Funktion:

1. Klicken Sie unter Windows oder macOS auf die **Passwortmanager** Symbol in Ihrem Webbrowser.
   Starten Sie unter Android oder iOS die **Passwortmanager** Anwendung.
   Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.
2. Öffnen Sie das Password Manager-Menü , um die Seitenleiste auf der linken Seite zu erweitern, und klicken Sie auf **Sichere mich** Menüpunkt.
3. Klicken Sie auf {1}Alle Sitzungen absichern{2}.

Wenn Sie nur ein einzelnes Gerät absichern möchten, suchen Sie es in der Liste der Geräte, auf denen der Password Manager installiert oder im Browser aktiviert ist.

4.3.4. Notizen

Die Funktion Sichere Notizen ist Ihr geheimes Notizbuch, in dem Sie vertrauliche Informationen speichern, ordnen und zur besseren Übersicht farblich kennzeichnen können. So sind die Informationen nicht nur gut organisiert, sondern auch sicher und vor fremden Zugriff geschützt.

So finden und aktivieren Sie diese Funktion:

1. Klicken Sie unter Windows oder macOS auf die **Passwortmanager** Symbol in Ihrem Webbrowser.
   Starten Sie unter Android oder iOS die **Passwortmanager** Anwendung.
   Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.
2. Öffnen Sie das Password Manager-Menü , um die Seitenleiste auf der linken Seite zu erweitern, und klicken Sie auf **Anmerkungen** Menüpunkt.
3. Drücken Sie auf die ⊕ **Hinweis hinzufügen** Taste.
   Wenn Sie die Informationen notiert haben, die Sie aufbewahren möchten, drücken Sie **Speichern**.

5. HÄUFIG GESTELLTE FRAGEN

Einige häufig gestellte Fragen zum Bitdefender Password Manager tauchen immer wieder auf. Wir haben die Antworten! Hier erfahren Sie mehr über Ihr Bitdefender-Konto, den Import von Passwörtern, Datensicherheitsprotokolle und andere für unsere Kunden wichtige Themen.

Allgemeine Fragen zum Bitdefender Password Manager

Wie stoppe ich das Password Manager-Popup in meiner Bitdefender-Sicherheitslösung?

Die im August 2022 von Bitdefender Total Security, Internet Security und Antivirus Plus angezeigte Password Manager-Benachrichtigung kann durch Klicken auf die Schaltfläche „x“ geschlossen werden. Das Fenster „Verwalten Sie Ihre Passwörter mit dem Bitdefender-Passwort-Manager“ wird nach dem Zufallsprinzip einige Male erneut angezeigt, bevor es für immer verschwindet. Sie können diese Werbenachricht abbestellen, indem Sie umschalten**Empfehlungsbenachrichtigungen**auf die Aus-Position in den Bitdefender-Einstellungen.

Was passiert, wenn der Bitdefender Password Manager abläuft?

Sobald Ihr Password Manager-Abonnement abläuft und nicht mehr aktiv ist, haben Sie maximal 90 Tage Zeit, um Ihre Passwörter zu exportieren. Ihre Passwörter werden für weitere 30 Tage gesichert. Während dieser 90 Tage können Sie Ihre Daten nur exportieren. Sie können Password Manager nicht weiter verwenden. Die Funktion zum automatischen Ausfüllen wird nicht mehr funktionieren, ebenso wie die Möglichkeit, Passwörter zu generieren.

Am Ende der 90-tägigen Nachfrist haben Sie 30 zusätzliche Tage Zeit, um den Bitdefender-Support zu kontaktieren und die Wiederherstellung Ihrer Passwörter in der Live-Datenbank anzufordern. Anschließend können Sie Ihre Passwörter aus Bitdefender Password Manager exportieren.

Ihre Daten werden nur bis zum Ende des Tages, an dem sie auf Anfrage wiederhergestellt wurden, in der Live-Datenbank aufbewahrt. Um Mitternacht wird die Datenbank gelöscht – und wenn Sie die 30-tägige Verlängerung noch nicht überschritten haben, können Passwörter

aus dem Backup wiederhergestellt werden. Datenbank-Rohdaten aus der Sicherung können dem Benutzer auf Anfrage zur Verfügung gestellt werden, aber die Datenbank ist verschlüsselt und auf die Informationen kann nicht zugegriffen werden.

Was ist ein Master-Passwort und warum muss ich es mir merken?

Das Master-Passwort ist der Schlüssel, der die Tür zu allen Passwörtern öffnet, die in Ihrem Bitdefender Password Manager-Konto gespeichert sind. Das Master-Passwort muss mindestens 8 Zeichen lang sein. Erstellen Sie also ein starkes Master-Passwort, merken Sie es sich und teilen Sie es niemals mit jemandem. Um ein starkes Master-Passwort zu erstellen, empfehlen wir Ihnen, eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (wie #, $ oder @) zu verwenden.

Wie kann ich verhindern, dass Bitdefender jedes Mal nach meinem Master-Passwort fragt, wenn ich den Browser öffne?

Wenn Sie Ihr Gerät sperren, ohne Ihren Browser zu schließen, wird Password Manager nicht gesperrt und Sie können auf Ihre Daten zugreifen, wenn Sie zurückkehren. Als Sicherheitsmaßnahme müssen Sie sich jedes Mal, wenn Sie den Browser öffnen, mit Ihrem Bitdefender Central-Konto anmelden und dann Ihr Master-Passwort eingeben.

- Um die zentrale Anmeldeaufforderung zu stoppen, gehen Sie zu ⚙ Einstellungen und aktivieren Sie „Registerkarte „Anmeldung beim Start deaktivieren“.
- Um die Eingabeaufforderung für das Master-Passwort zu beenden, aktivieren Sie das Kontrollkästchen „Remember me“ auf dem Bildschirm „Entsperren Sie Ihren Tresor“.

Warum speichern Sie mein Master-Passwort nicht und was passiert, wenn ich es vergesse?

Der Grund, warum wir Ihr Master-Passwort nicht auf unseren Servern speichern, ist, dass nur Sie auf Ihr Konto zugreifen können. Das ist der sicherste Weg. Wenn Bitdefender Password Manager Ihr Master-Passwort nicht erkennt, vergewissern Sie sich, dass Sie es richtig eingeben und dass die Feststelltaste auf der Tastatur nicht aktiv ist.

Wenn Sie das Master-Passwort vergessen, können Sie Password Manager jederzeit mit dem Wiederherstellungsschlüssel entsperren. Während des Anmeldevorgangs bietet Bitdefender Password Manager a

Wiederherstellungs-Schlüssel die verwendet werden können, um wieder Zugriff auf das Konto zu erhalten, ohne Ihre Daten zu verlieren.

Wenn Sie sowohl das Master-Passwort als auch den Wiederherstellungsschlüssel vergessen oder verlegt haben, wenden Sie sich als letzten Ausweg an einen Vertreter von Bitdefender, um Ihr Konto zurückzusetzen.

> **Wichtig**
> Durch das Zurücksetzen Ihres Kontos werden alle Ihre im Bitdefender Password Manager gespeicherten Daten und Passwörter gelöscht.

Können sich mehrere Benutzer ein Bitdefender Password Manager-Abonnement teilen?

Derzeit ist die Möglichkeit, mehrere Benutzer mit demselben Password Manager-Abonnement zu haben, nicht verfügbar, aber wir arbeiten daran, diese Funktion in naher Zukunft zu aktivieren.

Was ist der Offline-Modus und wie funktioniert er?

Der Offline-Modus wird automatisch aktiviert, wenn die Internetverbindung während der Verwendung von Bitdefender Password Manager unterbrochen wird. Wenn Sie bereits angemeldet sind und Ihr Master-Passwort eingegeben haben, können Sie im Offline-Modus auf Ihre Passwörter zugreifen, wenn keine Internetverbindung verfügbar ist.

Wie deinstalliere ich den Bitdefender Password Manager?

So deinstallieren Sie Bitdefender Password Manager:

- Unter Windows und macOS:
  Entfernen Sie die Password Manager-Erweiterung aus Ihrem Webbrowser. Klicken Sie mit der rechten Maustaste auf das Bitdefender-Symbol und wählen Sie „Entfernen“.
- Auf Android:
  Tippen und halten Sie die Password Manager-App und ziehen Sie sie dann an den oberen Rand des Bildschirms, wo „Deinstallieren“ steht.
- Unter iOS und iPadOS:
  Tippen und halten Sie die Password Manager-App, bis alle Apps auf Ihrem Bildschirm zu wackeln beginnen, und tippen Sie dann auf das X oben links neben dem Bitdefender-Symbol.

Datenschutz- und Sicherheitsfragen zum Bitdefender Password Manager

Können Bitdefender-Mitarbeiter meine Passwörter sehen?

Absolut nicht. Ihre Privatsphäre hat für uns oberste Priorität. Das ist der Hauptgrund, warum wir Ihr Master-Passwort nicht auf unseren Datenservern speichern: damit niemand Zugriff auf Ihr Konto hat, nicht einmal Mitarbeiter des Unternehmens. Jedes Passwort und Konto ist mit dem stärksten Datensicherheitsalgorithmus hochgradig verschlüsselt, und der Code, den wir sehen, sieht einfach aus wie eine zufällige Reihe von Zahlen und Buchstaben, die durcheinander gebracht werden.

Was würde passieren, wenn Password Manager-Server gehackt würden?

Jedes Passwort wird lokal auf Ihrem Gerät verschlüsselt, bevor es in die Nähe unserer Server gelangt. Wenn Hacker also in unser System eindringen würden, würden sie ohne Ihren Schlüssel nur Seiten mit zufälligen Buchstaben und Zahlen erhalten, um sie zu entschlüsseln. Das bedeutet, dass Sie und Ihre Kontodaten bei uns immer sicher sind.

6. HILFE BEKOMMEN

6.1. Hier wird Ihnen geholfen

Bitdefender bietet seinen Kunden einen konkurrenzlos schnellen und kompetenten Support. Wenn Sie ein Problem oder eine Frage zu Ihrem Bitdefender-Produkt haben, können Sie verschiedene Online-Ressourcen nutzen, um eine Lösung bzw. eine Antwort zu finden. Darüber hinaus können Sie sich jederzeit an den Bitdefender-Kundendienst wenden. Unsere Support-Mitarbeiter werden Ihre Fragen zeitnah beantworten und Ihnen die notwendige Unterstützung bieten.

Wenn Sie in den bereitgestellten Ressourcen keine Antwort auf Ihre Frage finden, können Sie uns auch direkt kontaktieren:

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

6.2. Online-Ressourcen

Bei Problemen und Fragen in Zusammenhang mit Bitdefender stehen verschiedene Online-Ressourcen zur Verfügung.

- Bitdefender-Support-Center:
  https://www.bitdefender.com/support/consumer.html
- Die Bitdefender Experten Community
  https://community.bitdefender.com
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

Weitere Informationen über Computersicherheit, Bitdefender-Produkte und unsere Firma finden Sie über Ihre Lieblingssuchmaschine.

6.2.1. Bitdefender-Support-Center

Das Bitdefender-Support-Center ist eine Online-Sammlung von Informationen zu Ihren Bitdefender-Produkten. Hier sind in einem leicht zugänglichen Format Berichte zu den Ergebnissen des fortlaufenden technischen Supports sowie der Bugfix-Aktivitäten der Bitdefender-Support- und Entwicklungsteams gespeichert. Hinzu kommen Artikel zur Bedrohungsvorbeugung, detaillierte Erklärungen zur Verwaltung von Bitdefender-Lösungen und vieles mehr.

Die Bitdefender Support Center ist zudem öffentlich zugänglich und komplett durchsuchbar. Durch diese Art der Informationsbereitstellung bieten wir unseren Kunden eine weitere Möglichkeit, technische Grundlagen und Fachwissen über unsere Produkte zu erlangen. Alle berechtigen Informationsanfragen oder Fehlermeldungen von Bitdefender-Kunden finden sich über kurz oder lang im Bitdefender Support Center wieder und dienen als Bugfix-Anleitungen, Umgehungslösungen oder Informationsartikel, die die Hilfedateien des Produkts ergänzen sollen.

Das Bitdefender Support Center ist jederzeit unter der folgenden Adresse erreichbar: https://www.bitdefender.com/support/consumer.html.

6.2.2. Die Bitdefender Experten Community

Die Experten-Community ist eine Plattform, auf der sich Bitdefender-Experten, -Anwender und -Fans einbringen, Ideen austauschen, sich gegenseitig unterstützen und ihr Wissen und ihre Lösungen mit anderen teilen. Hier werden zudem viele Ideen geboren und unsere Entwickler finden wichtiges Feedback. Unsere Community-Mitglieder sind erfahrene Bitdefender-Anwender, die Freude daran haben, anderen zu helfen. Dank ihres unschätzbaren Beitrags und ihres freiwilligen Engagements konnten wir eine Wissensdatenbank schaffen, in der Anwender nützliche Antworten und Anleitungen finden können, aber auch das Zwischenmenschliche seinen Platz hat.

Hier können Sie in einen echten Austausch mit Menschen treten, die Bitdefender selbst auf ihren Geräten nutzen. Die Community verbindet Sie mit unseren Mitgliedern und verschafft Ihrer Stimme Gehör. Hier werden Sie sich gerne einbringen, weil Sie wissen, dass Ihre Meinung und Ihr Beitrag respektiert und geschätzt werden. Als Anbieter Ihrer Wahl sind wir stets bestrebt, Ihnen beispiellos schnellen und kompetenten Support zu bieten und möchten Sie an unserer Seite wissen. Darum haben wir diese Community geschaffen.

Hier geht's zur Website unserer Expert Community:

https://community.bitdefender.com

6.2.3. Bitdefender Cyberpedia

In der Bitdefender Cyberpedia finden Sie alles Wissenswerte zu den neuesten Cyberbedrohungen. Hier teilen Bitdefender-Experten Tipps und

Tricks, wie Sie sich vor Hackern, Datenpannen, Identitätsdiebstahl und Identitätsbetrug in den sozialen Medien schützen können.

Die Bitdefender Cyberpedia finden Sie hier:

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

6.3. Kontaktinformation

Effiziente Kommunikation ist der Schlüssel zu einem erfolgreichen Unternehmen. Seit 2001 hat sich BITDEFENDER einen unbestreitbaren Ruf aufgebaut, indem es ständig nach besserer Kommunikation strebt, um die Erwartungen unserer Kunden und Partner zu übertreffen. Sollten Sie Fragen haben, zögern Sie nicht, uns direkt über unsere zu kontaktieren Bitdefender-Support-Center (Seite 33).

6.3.1. Lokale Vertriebspartner

Die Bitdefender Händler stehen für Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung, sowohl für vertriebliche als auch für allgemeine Anfragen.

So finden Sie einen Bitdefender Distributor in Ihrem Land:

1. Gehe zu https://www.bitdefender.com/partners/partner-locator.html.
2. Geben Sie über die entsprechenden Optionen Ihren Wohnort und Ihr Land an.

GLOSSAR

Aktivierungscode

Ist ein eindeutiger Schlüssel, der im Einzelhandel gekauft und zur Aktivierung eines bestimmten Produkts oder einer bestimmten Dienstleistung verwendet werden kann. Ein Aktivierungscode ermöglicht die Aktivierung eines gültigen Abonnements für einen bestimmten Zeitraum und eine bestimmte Anzahl von Geräten und kann auch zur Verlängerung eines Abonnements mit der zu generierenden Bedingung für dasselbe Produkt oder dieselbe Dienstleistung verwendet werden.

ActiveX

ActiveX ist ein Modell zum Schreiben von Programmen, damit andere Programme und das Betriebssystem sie aufrufen können. ActiveX-Technologie wird mit Microsoft Internet Explorer verwendet, um interaktive Webseiten zu erstellen, die wie Computerprogramme aussehen und sich verhalten und nicht wie statische Seiten. Mit ActiveX können Benutzer Fragen stellen oder beantworten, Schaltflächen verwenden und auf andere Weise mit der Webseite interagieren. ActiveX-Steuerelemente werden oft mit Visual Basic geschrieben. Active X zeichnet sich durch ein völliges Fehlen von Sicherheitskontrollen aus; Computersicherheitsexperten raten von der Verwendung über das Internet ab.

Fortgeschrittene anhaltende Bedrohung

Advanced Persistent Threat (APT) nutzt Schwachstellen von Systemen aus, um wichtige Informationen zu stehlen und an die Quelle zu liefern. Große Gruppen wie Organisationen, Unternehmen oder Regierungen werden von dieser Bedrohung angegriffen. Das Ziel einer Advanced Persistent Threat besteht darin, lange Zeit unentdeckt zu bleiben und wichtige Informationen zu überwachen und zu sammeln, ohne die Zielcomputer zu beschädigen. Die Methode, mit der die Bedrohung in das Netzwerk eingeschleust wird, erfolgt über eine harmlos aussehende PDF-Datei oder ein Office-Dokument, sodass jeder Benutzer die Dateien ausführen kann.

Adware

Adware wird oft mit einer Host-App kombiniert, die kostenlos zur Verfügung gestellt wird, solange der Benutzer zustimmt, die Adware zu

akzeptieren. Da Adware-Apps normalerweise installiert werden, nachdem der Benutzer einer Lizenzvereinbarung zugestimmt hat, in der der Zweck der App angegeben ist, liegt kein Verstoß vor. Popup-Werbung kann jedoch lästig werden und in einigen Fällen die Systemleistung beeinträchtigen. Außerdem können die Informationen, die einige dieser Apps sammeln, Datenschutzbedenken für Benutzer hervorrufen, die sich der Bedingungen in der Lizenzvereinbarung nicht vollständig bewusst waren.

Archiv

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einem Backup erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

Hintertür

Eine Lücke in der Sicherheit eines Systems, die von Designern oder Betreuern absichtlich hinterlassen wurde. Die Motivation für solche Löcher ist nicht immer finster; Einige Betriebssysteme sind zum Beispiel standardmäßig mit privilegierten Konten ausgestattet, die für die Verwendung durch Außendiensttechniker oder die Wartungsprogrammierer des Anbieters bestimmt sind.

Bootsektor

Ein Sektor am Anfang jeder Festplatte, der die Architektur der Festplatte identifiziert (Sektorgröße, Clustergröße usw.). Bei Startdisketten enthält der Bootsektor auch ein Programm, das das Betriebssystem lädt.

Boot-Virus

Eine Bedrohung, die den Bootsektor einer Festplatte oder Diskette infiziert. Ein Versuch, von einer Diskette zu booten, die mit einem Bootsektorvirus infiziert ist, führt dazu, dass die Bedrohung im Arbeitsspeicher aktiv wird. Jedes Mal, wenn Sie Ihr System ab diesem Zeitpunkt booten, ist die Bedrohung im Arbeitsspeicher aktiv.

Botnetz

Der Begriff „Botnet“ setzt sich aus den Wörtern „robot“ und „network“ zusammen. Botnets sind mit dem Internet verbundene Geräte, die mit Bedrohungen infiziert sind und dazu verwendet werden können, Spam-E-Mails zu versenden, Daten zu stehlen, anfällige Geräte fernzusteuern oder

Spyware, Ransomware und andere Arten von Bedrohungen zu verbreiten. Ihr Ziel ist es, so viele verbundene Geräte wie möglich zu infizieren, z. B. PCs, Server, mobile oder IoT-Geräte großer Unternehmen oder Branchen.

Browser

Abkürzung für Webbrowser, eine Software-App zum Auffinden und Anzeigen von Webseiten. Beliebte Browser sind Microsoft Internet Explorer, Mozilla Firefox und Google Chrome. Dies sind grafische Browser, was bedeutet, dass sie sowohl Grafiken als auch Text anzeigen können. Darüber hinaus können die meisten modernen Browser Multimedia-Informationen, einschließlich Sound und Video, darstellen, obwohl sie für einige Formate Plug-Ins benötigen.

Brute-Force-Angriff

Angriffe zum Erraten von Passwörtern wurden verwendet, um in ein Computersystem einzubrechen, indem mögliche Passwortkombinationen eingegeben wurden, meist beginnend mit dem am einfachsten zu erratenden Passwort.

Befehlszeile

In einer Befehlszeilenschnittstelle gibt der Benutzer Befehle unter Verwendung einer Befehlssprache direkt auf dem Bildschirm in den bereitgestellten Raum ein.

Kekse

In der Internetbranche werden Cookies als kleine Dateien beschrieben, die Informationen über einzelne Computer enthalten, die von Werbetreibenden analysiert und verwendet werden können, um Ihre Online-Interessen und Vorlieben zu verfolgen. In diesem Bereich wird die Cookie-Technologie noch entwickelt, und die Absicht besteht darin, Anzeigen direkt auf das auszurichten, was Sie als Ihre Interessen angegeben haben. Es ist für viele Menschen ein zweischneidiges Schwert, weil es einerseits effizient und relevant ist, da Sie nur Anzeigen zu dem sehen, woran Sie interessiert sind. Andererseits beinhaltet es tatsächlich das "Verfolgen" und "Folgen", wohin Sie gehen und worauf Sie klicken. Verständlicherweise gibt es eine Debatte über den Datenschutz und viele Menschen fühlen sich beleidigt von der Vorstellung, dass sie als „SKU-Nummer“ angesehen werden (Sie wissen schon, der Strichcode auf der Rückseite von Paketen, der an der Lebensmittelkasse gescannt wird). . Auch wenn dieser Standpunkt extrem sein mag, ist er in manchen Fällen richtig.

Cyber-Mobbing

Wenn Gleichaltrige oder Fremde absichtlich missbräuchliche Handlungen gegen Kinder begehen, um sie körperlich zu verletzen. Um emotional zu schädigen, senden die Angreifer gemeine Nachrichten oder wenig schmeichelhafte Fotos, wodurch ihre Opfer von anderen isoliert werden oder sich frustriert fühlen.

Wörterbuchangriff

Bei Angriffen zum Erraten von Passwörtern wurde früher in ein Computersystem eingebrochen, indem eine Kombination gängiger Wörter eingegeben wurde, um potenzielle Passwörter zu generieren. Das gleiche Verfahren wird verwendet, um Entschlüsselungsschlüssel von verschlüsselten Nachrichten oder Dokumenten zu erraten. Wörterbuchangriffe sind erfolgreich, weil viele Menschen dazu neigen, kurze und aus einzelnen Wörtern bestehende Passwörter zu wählen, die leicht zu erraten sind.

Laufwerk

Es ist eine Maschine, die Daten von einer Festplatte liest und auf diese schreibt. Ein Festplattenlaufwerk liest und beschreibt Festplatten. Ein Diskettenlaufwerk greift auf Disketten zu. Laufwerke können entweder intern (in einem Computer untergebracht) oder extern (in einem separaten Gehäuse untergebracht, das mit dem Computer verbunden ist) sein.

Herunterladen

Kopieren von Daten (normalerweise eine ganze Datei) von einer Hauptquelle auf ein Peripheriegerät. Der Begriff wird häufig verwendet, um den Vorgang des Kopierens einer Datei von einem Onlinedienst auf den eigenen Computer zu beschreiben. Herunterladen kann sich auch auf das Kopieren einer Datei von einem Netzwerkdateiserver auf einen Computer im Netzwerk beziehen.

Email

E-Mail. Ein Dienst, der Nachrichten auf Computern über lokale oder globale Netzwerke sendet.

Veranstaltungen

Eine Aktion oder ein Ereignis, das von einem Programm erkannt wird. Ereignisse können Benutzeraktionen sein, wie z. B. das Klicken auf eine Maustaste oder das Drücken einer Taste, oder Systemvorfälle, wie z. B. Speichermangel.

Exploits

Eine Möglichkeit, verschiedene Bugs oder Schwachstellen auszunutzen, die in einem Computer (Software oder Hardware) vorhanden sind. Somit können Hacker die Kontrolle über Computer oder Netzwerke erlangen.

Falsch positiv

Tritt auf, wenn ein Scanner eine Datei als infiziert identifiziert, obwohl dies nicht der Fall ist.

Dateinamenerweiterung

Der Teil eines Dateinamens nach dem letzten Punkt, der die Art der in der Datei gespeicherten Daten angibt. Viele Betriebssysteme verwenden Dateinamenerweiterungen, z. B. Unix, VMS und MS-DOS. Sie bestehen normalerweise aus einem bis drei Buchstaben (einige traurige alte Betriebssysteme unterstützen nicht mehr als drei). Beispiele sind „c“ für C-Quellcode, „ps“ für PostScript, „txt“ für beliebigen Text.

Heuristik

Eine regelbasierte Methode zur Identifizierung neuer Bedrohungen. Diese Scanmethode ist nicht auf eine Datenbank mit spezifischen Bedrohungsinformationen angewiesen. Der Vorteil des heuristischen Scans besteht darin, dass er nicht von einer neuen Variante einer bestehenden Bedrohung getäuscht wird. Es kann jedoch gelegentlich verdächtigen Code in normalen Programmen melden, wodurch das sogenannte "Falsch-Positive" generiert wird.

Honigtopf

Ein Köder-Computersystem, das Hacker dazu bringen soll, ihre Vorgehensweise zu studieren und die ketzerischen Methoden zu identifizieren, mit denen sie Systeminformationen sammeln. Unternehmen und Konzerne sind mehr daran interessiert, Honeypots zu implementieren und zu nutzen, um ihren allgemeinen Sicherheitszustand zu verbessern.

IP

Internet Protocol – Ein routingfähiges Protokoll in der TCP/IP-Protokollfamilie, das für die IP-Adressierung, das Routing und die Fragmentierung und Wiederzusammensetzung von IP-Paketen verantwortlich ist.

Java-Applet

Ein Java-Programm, das nur für die Ausführung auf einer Webseite konzipiert ist. Um ein Applet auf einer Webseite zu verwenden, würden Sie den Namen des Applets und die Größe (Länge und Breite in Pixeln) angeben, die das Applet verwenden kann. Wenn auf die Webseite zugegriffen wird, lädt der Browser das Applet von einem Server herunter und führt es auf dem Computer des Benutzers (dem Client) aus. Applets unterscheiden sich von Apps dadurch, dass sie einem strengen Sicherheitsprotokoll unterliegen.

Obwohl beispielsweise Applets auf dem Client ausgeführt werden, können sie keine Daten auf dem Computer des Clients lesen oder darauf schreiben. Darüber hinaus werden Applets weiter eingeschränkt, sodass sie nur Daten aus derselben Domäne lesen und schreiben können, von der sie bedient werden.

Keylogger

Ein Keylogger ist eine App, die alles protokolliert, was Sie eingeben. Keylogger sind von Natur aus nicht bösartig. Sie können für legitime Zwecke verwendet werden, z. B. zur Überwachung der Aktivitäten von Mitarbeitern oder Kindern. Sie werden jedoch zunehmend von Cyberkriminellen für böswillige Zwecke verwendet (z. B. um private Daten wie Anmeldedaten und Sozialversicherungsnummern zu sammeln).

Makrovirus

Eine Art von Computerbedrohung, die als in ein Dokument eingebettetes Makro codiert ist. Viele Apps wie Microsoft Word und Excel unterstützen leistungsstarke Makrosprachen. Mit diesen Apps können Sie ein Makro in ein Dokument einbetten und das Makro jedes Mal ausführen, wenn das Dokument geöffnet wird.

Mail-Client

Ein E-Mail-Client ist eine Anwendung, mit der Sie E-Mails senden und empfangen können.

Speicher

Interne Speicherbereiche im Computer. Der Begriff Speicher bezeichnet Datenspeicher in Form von Chips, und das Wort Speicher wird für Speicher verwendet, der auf Bändern oder Platten vorhanden ist. Jeder Computer verfügt über eine bestimmte Menge an physischem Speicher, der normalerweise als Hauptspeicher oder RAM bezeichnet wird.

Nicht heuristisch

Diese Scanmethode stützt sich auf eine Datenbank mit spezifischen Bedrohungsinformationen. Der Vorteil des nicht-heuristischen Scans besteht darin, dass er nicht durch scheinbare Bedrohungen getäuscht wird und keine Fehlalarme erzeugt.

Online-Raubtiere

Personen, die versuchen, Minderjährige oder Heranwachsende absichtlich in Gespräche zu verwickeln, um sie in illegale sexuelle Aktivitäten zu verwickeln. Soziale Netzwerke sind der ideale Ort, an dem gefährdete Kinder leicht gejagt und zu sexuellen Aktivitäten verführt werden können, online oder von Angesicht zu Angesicht.

Gepackte Programme

Eine Datei in einem komprimierten Format. Viele Betriebssysteme und Apps enthalten Befehle, mit denen Sie eine Datei so packen können, dass sie weniger Speicherplatz beansprucht. Angenommen, Sie haben eine Textdatei mit zehn aufeinanderfolgenden Leerzeichen. Normalerweise würde dies zehn Bytes Speicherplatz erfordern.

Ein Programm, das Dateien packt, würde jedoch die Leerzeichen durch ein spezielles Leerzeichen ersetzen, gefolgt von der Anzahl der zu ersetzenden Leerzeichen. In diesem Fall würden die zehn Leerzeichen nur zwei Bytes erfordern. Dies ist nur eine Verpackungstechnik – es gibt noch viele mehr.

Weg

Die genauen Anweisungen zu einer Datei auf einem Computer. Diese Richtungen werden in der Regel durch das hierarchische Ablagesystem von oben nach unten beschrieben.

Die Route zwischen zwei beliebigen Punkten, z. B. der Kommunikationskanal zwischen zwei Computern.

Phishing

Das Senden einer E-Mail an einen Benutzer, der fälschlicherweise vorgibt, ein etabliertes legitimes Unternehmen zu sein, um den Benutzer dazu zu bringen, private Informationen preiszugeben, die für Identitätsdiebstahl verwendet werden. Die E-Mail leitet den Benutzer an, eine Website zu besuchen, auf der er aufgefordert wird, persönliche Informationen wie Passwörter und Kreditkarten-, Sozialversicherungs- und Bankkontonummern zu aktualisieren, die die legitime Organisation bereits

hat. Die Website ist jedoch gefälscht und nur dazu eingerichtet, die Informationen des Benutzers zu stehlen.

Photon

Photon ist eine innovative, nicht-intrusive Bitdefender-Technologie, die entwickelt wurde, um die Auswirkungen auf die Leistung Ihrer Sicherheitslösung zu minimieren. Durch die Überwachung der Aktivitäten Ihres PCs im Hintergrund werden Nutzungsmuster erstellt, die dabei helfen, Boot- und Scan-Prozesse zu optimieren.

Polymorphes Virus

Eine Bedrohung, die ihre Form mit jeder Datei, die sie infiziert, ändert. Da diese Bedrohungen kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Hafen

Eine Schnittstelle an einem Computer, an die ein Gerät angeschlossen werden kann. PCs haben verschiedene Arten von Anschlüssen. Intern gibt es mehrere Anschlüsse für den Anschluss von Laufwerken, Bildschirmen und Tastaturen. Extern haben PCs Anschlüsse für den Anschluss von Modems, Druckern, Mäusen und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen.Die Schnittstellennummer gibt die Art der Schnittstelle an.Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Ransomware

Ransomware ist bösartige Software, die das System des Opfers sperrt und nur gegen ein Lösegeld wieder entfernt wird. CryptoLocker, CryptoWall und TeslaWall sind einige bekanntere Beispiele für Ransomware.

Die Infektion kann sich durch das Aufrufen eine Spam-Nachricht, das Herunterladen eines E-Mail-Anhangs oder die Installation von Anwendungen ausbreiten, ohne dass der Benutzer es überhaupt bemerkt. Ransomware-Hacker nehmen herkömmliche Benutzer und Unternehmen ins Visier.

Datei melden

Eine Datei, die stattgefundene Aktivitäten aufzeichnet.Zum Beispiel speichert BitDefender eine Logdatei mit die geprüften Pfaden, Ordnern und der Archivanzahl, aber auch die geprüften, infizierten oder verdächtigen Dateien.

Rootkit

Ein Rootkit ist eine Sammlung von Software-Tools, die den Zugriff auf ein System auf Administratorebene ermöglichen. Der Begriff wurde erstmals für UNIX-Betriebssysteme verwendet und bezog sich auf neu kompilierte Tools, die Eindringlingen administrative Rechte verschafften und es ihnen ermöglichten, ihre Anwesenheit zu verbergen, um der Erkennung durch den Systemadministrator zu entgehen.

Die Hauptaufgabe von Rootkits besteht darin, Prozesse, Dateien, Logins und Protokolle zu verbergen. Sie können auch Daten von Terminals, Netzwerkverbindungen oder Peripheriegeräten abfangen, wenn sie die entsprechende Software enthalten.

Rootkits sind nicht grundsätzlich schädlich. Einige Systeme und Anwendungen verstecken z. B. wichtige Dateien mithilfe von Rootkits. Sie werden jedoch oft dazu missbraucht, Bedrohungen zu verbergen oder unbemerkt einen Eindringling einzuschleusen. In Kombination mit anderen Bedrohungen stellen Rootkits eine große Gefahr für Ihr System dar. Denn sie können den Datenverkehr abhören, Sicherheitslücken in Ihrem System schaffen, Dateien und Zugangsdaten verändern, und das alles, ohne entdeckt zu werden.

Skript

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Beiträge in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten über seine Internetverbindung abgreift. Dies geschieht in der Regel zu Werbezwecken. Typischerweise sind Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Shareware-Programmen enthalten, die aus dem Internet heruntergeladen werden können. Die große Mehrzahl von Shareware- und Freeware-Anwendungen ist natürlich frei von Spyware. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an einen Dritten. Spyware kann auch Informationen über E-Mail-Adressen und sogar Passwörter und Kreditkartennummern sammeln.

Einer Bedrohung durch ein trojanisches Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Opfer von Spyware wird man oft dann, wenn man sich bestimmte Peer-to-Peer-Dateiaustauschprogramme herunterlädt.

Ganz abgesehen von den Fragen der Ethik und des Datenschutzes belegt Spyware auch unnötig Systemressourcen und Bandbreite, indem über die Internetverbindung des Nutzers Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Startobjekte

Jede Datei, die sich in diesem Ordner befindet, wird geöffnet, wenn der Rechner gestartet wird. Das können z. B. ein Startbildschirm, eine Sounddatei, die beim Systemstart abgespielt wird, ein Erinnerungskalender oder auch Apps sein. Gewöhnlich wird eine Alias-Datei (Verknüpfung) statt der eigentlichen Datei in diesen Ordner gelegt.

Abonnement

Ein Kaufvertrag, der Benutzern das Recht einräumt, ein bestimmtes Produkt oder eine Dienstleistung auf einer bestimmten Anzahl von Geräten und für einen bestimmten Zeitraum in Anspruch zu nehmen. Ein abgelaufenes Abonnement kann unter Verwendung der vom Nutzer beim Ersterwerb angegebenen Informationen automatisch verlängert werden.

System Tray

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Taskleiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Sie enthält kleine Icons zur Information und zum leichteren Zugriff, zum Beispiel: Fax, Drucker, Modem, Lautstärke und mehr. Um auf die Details und Steuerungen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol – im Internet weit verbreiteter Netzwerkprotokollsatz, der die Kommunikation zwischen verbundenen Computernetzwerken mit verschiedenen Hardware-Architekturen und Betriebssystemen ermöglicht. TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Gefahr

Ein Programm oder ein Stück Code, das auf einen Rechner kopiert wird und sich allein ausführt, ohne dass es der Besitzer des Rechners will oder merkt. Die meisten Bedrohungen können sich auch selbst vervielfältigen. Alle Computerbedrohungen wurden von Menschen programmiert. Eine einfache Bedrohung, die sich immer wieder vervielfältigen kann, ist sehr einfach zu programmieren. Sogar eine solch einfache Bedrohung kann gefährlich sein, da sie im Handumdrehen sämtlichen Arbeitsspeicher belegen und so das System lahmlegen kann. Noch gefährlicher sind Bedrohungen, die sich über Netzwerke hinweg selbst weiterversenden und Sicherheitssysteme umgehen.

Aktualisierung der Bedrohungsinformationen

Das binäre Muster einer Bedrohung, wird von der Sicherheitslösung zur Erkennung und Beseitigung einer Bedrohung genutzt.

Trojaner

Ein bösartiges Programm, das sich als eine legitime Anwendung ausgibt. Anders als Schad-Software und Würmer vervielfältigen sich Trojaner nicht selbst, können aber dennoch großen Schaden anrichten. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Bedrohungen zu befreien, stattdessen aber den Rechner infiziert.

Der Begriff entstammt einer Geschichte in Homer's "Ilias", in der die Griechen Ihren Feinden, den Trojanern, angeblich als Sühnegabe ein hölzernes Pferd schenkten.Aber, nachdem die Trojaner das Pferd innerhalb der Stadtmauern gebracht hatten, kamen die in dem Bauch des hölzernen Pferdes versteckten Soldaten heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsmännern in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Aktualisieren

Neue Softwareversionen oder Hardwareprodukte, die eine ältere Version ersetzen.Die Update-Installationsroutine sucht nach älteren Versionen auf dem Rechner, da sonst kein Update installiert werden kann.

Bitdefender verfügt über eine eigene Update-Funktion, über die Sie manuell nach Updates suchen oder das Produkt automatisch aktualisieren lassen können.

Virtuelles privates Netzwerk (VPN)

Mit dieser Technologie ist es möglich, eine zeitlich begrenzte und verschlüsselte direkte Verbindung mit einem bestimmten Netzwerk auch über ein weniger gut gesichertes Netzwerk aufzubauen. Auf diese Weise können Daten sicher und verschlüsselt versandt und empfangen werden und sind für neugierige Augen nur schwer einsehbar. Bei einem Sicherheitsnachweis handelt es sich um eine Authentifizierung, die ausschließlich über einen Benutzernamen und ein Passwort erfolgen kann.

Wurm

Ein Programm, das sich selbst über ein Netzwerk ausbreitet und sich dabei selbst reproduziert. Es kann sich nicht an andere Programme anhängen.