GEBRUIKSAANWIJZING

Bitdefender CONSUMER SOLUTIONS

SecurePass

Bitdefender SecurePass

Handleiding

Publication date 20/11/2024

Juridische kennisgeving

Bitdefender

Inhoudsopgave

OVER DEZE GIDS

Voor wie is deze handleiding bedoeld?

Deze gids is bedoeld voor alle Bitdefender-gebruikers op alle ondersteunde besturingssystemen (Windows, MacOS, Android, iOS) die Bitdefender SecurePass hebben gekozen als hun favoriete instrument voor wachtwoordbeheer. De informatie in dit boek is niet alleen geschikt voor computergebruikers, maar dient als een toegankelijke en handige gids voor iedereen.

Deze gids helpt u te ontdekken hoe u het beste kunt halen uit onze ultra-veilige wachtwoordmanager met talloze functies. Alle kenmerken en functionaliteiten worden er in detail in besproken.

Wij wensen u veel aangenaam en nuttig leesplezier.

Hoe kunt u deze handleiding gebruiken?

De handleiding is ingedeeld aan de hand van enkele hoofdonderwerpen:

Aan de slag (pagina 5)

Ga aan de slag met Bitdefender SecurePass en het installatieproces.

Uw wachtwoorden importeren en exporteren (pagina 10)

Begrijp hoe u wachtwoorden in en uit SecurePass kunt importeren of exporteren.

Kenmerken en functionaliteiten (pagina 14)

Leer hoe u Bitdefender SecurePass en al zijn functies gebruikt.

Hulp vragen (pagina 26)

Informatie over waar u om hulp kunt vragen indien er zich onverwachte problemen voordoen.

Conventies die in deze gids worden gebruikt

Typografische conventies

In deze gids worden verschillende tekststijlen gebruikt, zodat de tekst leesbaarder is. De weergave en betekenis worden in de onderstaande tabel voorgesteld.

Weergave	Beschrijving
voorbeeld-syntaxis	Voorbeelden van syntaxis worden weergegeven in een niet-proportioneel lettertype.
https://www.bitdefender.com	De URL-koppeling wijst naar een externe locatie op http- of ftp-servers.
documentation@bitdefender.com	E-mailadressen worden in de tekst ingevoegd voor contactgegevens.
Over deze gids (pagina 1)	Dit is een interne koppeling naar een locatie in het document.
bestandsnaam	Namen van bestanden en mappen worden weergegeven in een niet-proportioneel lettertype.
optie	Alle productopties worden **vet** weergegeven.
trefwoord	Sleutelwoorden en belangrijke zinsdelen worden **vet** weergegeven.

Waarschuwingen

De waarschuwingen zijn grafisch gemarkeerde opmerkingen in de tekst die extra informatie over de huidige paragraaf onder de aandacht brengen.

Opmerking

De opmerking is slechts een kort commentaar. Hoewel u opmerkingen kunt weglaten, kunnen ze toch waardevolle informatie bieden zoals over een specifieke functie of een koppeling naar een verwant onderwerp.

Belangrijk

Dit vereist uw aandacht en het wordt niet aanbevolen dit te negeren. Doorgaans betreft het niet-kritieke, maar belangrijke informatie.

Waarschuwing

Dit is kritische informatie die u aandachtig moet lezen. Er zullen geen ernstige problemen optreden als u de aanwijzingen volgt. U moet de informatie lezen en begrijpen omdat hier iets wordt beschreven dat hoge risico's inhoudt.

Verzoek om commentaar

We willen u uitnodigen ons te helpen dit boek te verbeteren. Wij hebben alle informatie zo goed mogelijk getest en gecontroleerd. Laat ons weten of u enige tekortkomingen hebt ontdekt in dit boek of als u ideeën hebt om dit te verbeteren, zodat wij u de best mogelijke documentatie kunnen bieden.

U kunt contact met ons opnemen door een e-mail te sturen naar documentation@bitdefender.com. Wij verzoeken u al uw e-mails met

betrekking tot de documentatie in het Engels te schrijven, zodat we uw opmerkingen op een efficiënte manier kunnen verwerken.

1. WAT IS BITDEFENDER SECUREPASS

Bitdefender SecurePass is een multi-platform dienst ontworpen om gebruikers te helpen bij het opslaan en organiseren van al hun online wachtwoorden. Het is gebouwd met de sterkste bekende cryptografische algoritmen voor het hoogste niveau van veiligheid en digitale beveiliging. Het werkt als een browserextensie en mobiele app-oplossing voor identiteits- en wachtwoordbeheer, bankieren en alle andere soorten gevoelige informatie op verschillende apparaten.

Bitdefender SecurePass kan uw wachtwoorden automatisch opslaan, invullen, genereren en beheren voor alle websites en online diensten met behulp van een enkel hoofdwachtwoord, waardoor uw digitale identiteit in het algemeen veel gemakkelijker te beheren is.

1.1. Proef- en betaalde versies van Password Manager

De proefversie van Bitdefender Password Manager werkt op alle accounts op dezelfde manier als de betaalde versie van het product, maar de beschikbaarheid ervan vervalt 90 dagen na activering.

Opmerking

Merk op dat de betaalde versie van het product weliswaar kan worden gekocht als een puur standalone product, maar dat onbeperkte toegang tot Password Manager is inbegrepen in de abonnementen Bitdefender Premium Security en Bitdefender Ultimate Security.

2. AAN DE SLAG

2.1. Systeemvereisten

U kunt de laatste versie van Bitdefender SecurePass alleen gebruiken op apparaten met de volgende besturingssystemen:

- **Voor pc-gebruikers:**
  - Windows 7 met Service Pack 1
  - Windows 8.1
  - Windows 10
  - Windows 11
- **Voor macOS-gebruikers:**
  - macOS 10.14 (Mojave) en recentere macOS-besturingssystemen

  Opmerking
  Merk op dat de systeemprestaties kunnen worden beïnvloed op apparaten met CPU's van een oudere generatie.
- **Voor iOS-gebruikers:**
  - iOS 11.0 of recentere iOS-besturingssystemen
- **Voor Android-gebruikers:**
  - Android 5.1 en recentere Android-besturingssystemen

  Opmerking
  - Vingerafdrukontgrendeling wordt ondersteund op **Android 6.0** en hoger.
  - De functie automatisch invullen wordt ondersteund op **Android 8.0** en hoger, en is compatibel met iPhone, iPad en iPod touch.

2.1.1. Softwarevereisten

Om Bitdefender SecurePass en al zijn functies te kunnen gebruiken, moeten uw Windows- of macOS-apparaten aan de volgende softwarevereisten voldoen:

- **Microsoft Edge** (gebaseerd op Chromium 80 en hoger)
- **Mozilla Firefox** (versie 65 of hoger)
- **Google Chrome** (versie 72 of hoger)
- **Safari** (versie 12 of hoger)

Opmerking
De software-vereisten zijn niet van toepassing voor Android en iOS.

Waarschuwing
Het niet voldoen aan de bovenstaande systeemvereisten heeft tot gevolg dat Bitdefender SecurePass niet kan worden geïnstalleerd of dat het product niet goed functioneert.

2.2. Installatie

In dit hoofdstuk wordt uitgelegd hoe u Bitdefender SecurePass installeert op zowel de webbrowsers op uw Windows pc en macOS, als op uw mobiele Android- of iOS-apparaten.

Belangrijk
Zorg er vóór de installatie voor dat u een geldig Password Manager-abonnement hebt in uw **Bitdefender Central**-account, zodat deze browserextensie de geldigheid ervan kan ophalen uit uw account.

Actieve abonnementen worden weergegeven in het onderdeel **Mijn abonnementen** in Bitdefender Central.

2.2.1. Installatie op Windows- en macOS-apparaten

In tegenstelling tot de meeste desktoptoepassingen en software die geïnstalleerd en ingesteld moeten worden op deze apparaten, wordt Bitdefender Password Manager geleverd als een browserextensie - ook wel add-on genoemd - die snel kan worden toegevoegd en ingeschakeld in de browser van uw voorkeur.

De momenteel ondersteunde browsers voor het product zijn de volgende: **Google Chrome**, **Mozilla Firefox**, **Microsoft Edge**, en **Safari**.

- **Google Chrome**
- **Mozilla Firefox**

- **Microsoft Edge**
- **Safari**

Om Bitdefender SecurePass te installeren:

1. Volg na aankoop van Bitdefender SecurePass de stappen in de bevestigingsmail om uw abonnement te activeren.
2. Meld u aan bij Bitdefender Central met uw inloggegevens.
   Selecteer in het menu aan de linkerkant **SecurePass**.
3. Selecteer in het SecurePass-paneel de browser van uw voorkeur.
4. Installeer de browserextensie:

   - **Google Chrome:**
     a. Klik op de **Aan Chrome toevoegen** knop.
     b. Klik in het bevestigingsvenster op **Extensie toevoegen**.

   - **Mozilla Firefox:**
     a. Klik op de **Aan Firefox toevoegen** knop.
     b. Klik op de **Installeren** knop in de rechterbovenhoek van het scherm.

   - **Microsoft Edge:**
     a. Klik op de **Krijg** knop.
     b. Klik **Extensie toevoegen** in de prompt die verschijnt.

   - **Safari:**
     a. Het SecurePass-installatieprogramma wordt gedownload naar uw macOS-apparaat. Dubbelklik op het gedownloade bestand en volg vanaf daar de instructies op het scherm
     b. Open aan het einde van het installatieproces de **Safari** browser en selecteer **Voorkeuren** in de bovenste menubalk.
     c. Klik in de Voorkeurenvensters op de **Tabblad Extensies**.
     d. Vink het vakje aan naast **Bitdefender SecurePass** om het mogelijk te maken.

Nadat de extensie is geïnstalleerd, kunt u doorgaan naar het Installatieproces (pagina 9).

2.2.2. Installatie op Android-apparaten

De eenvoudigste manier om Bitdefender Password Manager voor Android-telefoons en -tablets te installeren, is door de applicatie rechtstreeks van Google Play te downloaden.

1. Zorg ervoor dat u na de aankoop eerst de bevestigingsmail opent die u hebt ontvangen om de instructies te volgen die u daar vindt om uw SecurePass-abonnement te activeren.
2. Open de Google Play Store op je Android-apparaat.
3. Typ in de zoekbalk van de Google Play Store **Bitdefender SecurePass**, zoek en download de applicatie.
4. Zodra de download is voltooid, opent u de app en volgt u, indien nodig, de configuratiestappen op het scherm die nodig zijn om het installatieproces te voltooien.

De installatie op uw Android-apparaat is nu voltooid.

2.2.3. Installatie op iOS-apparaten

De eenvoudigste manier om Bitdefender Password Manager voor iOS- en iPadOS-apparaten te installeren, is door de applicatie te downloaden van de Apple App Store.

1. Zorg ervoor dat u na de aankoop eerst de bevestigingsmail opent die u hebt ontvangen om de instructies te volgen die u daar vindt om uw SecurePass-abonnement te activeren.
2. Open de App Store op je iOS-apparaat.
3. Typ in de zoekbalk van de App Store **Bitdefender SecurePass**, zoek en download de applicatie.
4. Zodra de download is voltooid, opent u de app en volgt u, indien nodig, de configuratiestappen op het scherm die nodig zijn om het installatieproces te voltooien.

De installatie op uw iOS- / iPadOS-apparaat is nu voltooid.

2.3. Installatieproces

Om Bitdefender SecurePass in te stellen op uw browser/mobiele apparaat:

1. Na het voltooien van het installatieproces opent u de SecurePass-extensie/toepassing en logt u in.
   Gebruik de inloggegevens van het Bitdefender-account dat is gekoppeld aan uw SecurePass-abonnement.
2. U wordt gevraagd om een **Hoofdwachtwoord**.

   > **Belangrijk**
   > Houd er rekening mee dat u dit hoofdwachtwoord nodig hebt om alle wachtwoorden, creditcardgegevens en notities te ontgrendelen die zijn opgeslagen in Bitdefender SecurePass. Dit is in wezen de sleutel waarmee de eigenaar dit product kan gebruiken.

   Zorg ervoor dat u een sterk hoofdwachtwoord invoert zonder het risico te lopen dat u het gemakkelijk vergeet.
   Zodra u een sterk en uniek hoofdwachtwoord hebt gekozen, klikt u op **Opslaan en doorgaan**.
3. Vervolgens krijgt u een **Herstelsleutel**.

   > **Waarschuwing**
   > Na het aanmaken van het hoofdwachtwoord ontvangt u een **24-cijferige herstelsleutel**. Noteer uw herstelsleutel op een veilige plaats en raak deze niet kwijt. Deze sleutel is de enige manier om toegang te krijgen tot uw wachtwoorden die zijn opgeslagen in Password Manager voor het geval u **vergeet het hoofdwachtwoord** eerder ingesteld voor je account.

   - Sla de herstelsleutel op door deze naar uw klembord te kopiëren of als PDF-bestand te downloaden.
     Je kunt op drukken **Sluiten** als je klaar bent.
4. Als u klaar bent, selecteert u de **Toegang tot je kluis** knop.

Nu het installatieproces is voltooid, kunt u Bitdefender SecurePass gaan gebruiken.

3. UW WACHTWOORDEN IMPORTEREN EN EXPORTEREN

Bitdefender Password Manager is zo gebouwd dat communicatie en gegevensoverdracht met externe bronnen, platforms en softwaretools efficiënt verlopen. Dit is de belangrijkste reden waarom met gemak kan worden voldaan aan de zeer vaak voorkomende nood aan het importeren of exporteren van wachtwoorden in of uit Bitdefender Password Manager.

3.1. Compatibiliteit

Bitdefender Password Manager kan naadloos gegevens overdragen van de volgende lijst van applicaties:

- Bitdefender wachtwoordbeheerder
- Bitdefender-portemonnee
- Bitdefender SecurePass
- SaferPass
- 1 wachtwoord
- Kaspersky
- Dashlane
- Chrome-browser
- Firefox-browser
- Microsoft Edge
- Bitwarden
- LastPass
- KeePass
- RoboForm

Deze overdracht van gegevens tussen Bitdefender Password Manager en andere software voor accountbeheer kan gebeuren via de volgende gegevensformaten:

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

3.2. Importeren in Password Manager

Met Bitdefender Password Manager kunt u gemakkelijk wachtwoorden importeren uit andere wachtwoordbeheerders en browsers. Als u momenteel wilt overstappen naar Bitdefender Password Manager vanuit een andere dienst voor wachtwoordbeheer, hebt u waarschijnlijk een aanzienlijke hoeveelheid gegevens opgeslagen, zoals gebruikersnamen, wachtwoorden en andere aanmeldingsgegevens die nodig zijn voor al uw accounts.

Nu u Bitdefender Password Manager hebt gekozen, kunt u de opgeslagen gegevens erin importeren.

Hier leest u hoe u uw opgeslagen informatie van andere apps en webbrowsers kunt importeren in Bitdefender Password Manager, **ongeacht het besturingssysteem** waarop u dit product hebt geïnstalleerd:

1. Open Bitdefender SecurePass en ga naar **Instellingen**.
   - In de browser:
     Klik op **Instellingen** in de rechterbovenhoek van de pagina.
   - In de app:
     Tik op de **Meer** knop in de rechteronderhoek van het scherm en tik bovenaan de lijst die daarna verschijnt op **Instellingen**.
2. In het **Back-up maken en herstellen** sectie, selecteer **Wachtwoorden importeren**. Het importvenster wordt geopend.
3. Selecteer de naam van de wachtwoordbeheerder of webbrowser die u eerder hebt gebruikt in het keuzemenu dat toegankelijk is via de **Selecteer het bestandstype** veld.

   > **Opmerking**
   > Als er een wachtwoord is gebruikt om het bestand te versleutelen, moet u dit invoeren in het **Wachtwoord** veld; anders kunt u het leeg laten.

4. Selecteer de **Selecteer het bestand om te importeren** gearchiveerd.
   Navigeer naar de locatie waar de geëxporteerde gegevens van uw oude wachtwoordbeheerder zijn opgeslagen. Kies het bestand zodra je het hebt gevonden en klik vervolgens op **Open**.

5. Nadat u het bestand hebt geselecteerd, selecteert u **Importeren** in de linkeronderhoek van het importvenster. Het proces begint binnenkort, vergezeld van een voortgangsbalk.

Na het importeren worden uw wachtwoorden toegankelijk op alle apparaten waarop de toepassing Bitdefender Password Manager of de browserextensie is geïnstalleerd.

> **Opmerking**
> Als u teruggaat naar uw wachtwoordkluis in SecurePass, ziet u een map met de naam **Importeren**, met alle gegevens van uw vorige wachtwoordbeheerder of webbrowser.

3.3. Exporteren vanuit Password Manager

Met Bitdefender Password Manager kunt u gemakkelijk uw opgeslagen wachtwoorden (inclusief account-logins, beveiligde notities, enz.) exporteren naar een CSV-bestand (door komma's gescheiden waarden) of een gecodeerd bestand als u ooit wilt overschakelen naar een andere wachtwoordbeheerdienst, zodat uw vertrek van Bitdefender Password Manager geen moeilijk proces zal zijn.

> **Belangrijk**
> Een CSV-bestand is **niet** versleuteld en bevat gebruikersnamen en wachtwoorden in platte tekst, wat betekent dat uw privégegevens kunnen worden gelezen door iedereen die toegang heeft tot uw apparaat. Wij raden u daarom aan de onderstaande instructies te volgen op een vertrouwd apparaat.

Hier leest u hoe u uw gegevens uit Bitdefender Password Manager kunt exporteren:

1. Open Bitdefender SecurePass en ga naar **Instellingen**.
   - In de browser:
     Klik op **Instellingen** in de rechterbovenhoek van de pagina.
   - In de app:
     Tik op de **Meer** knop in de rechteronderhoek van het scherm en tik bovenaan de lijst die daarna verschijnt op **Instellingen**.
2. In het **Back-up maken en herstellen** sectie, selecteer **Wachtwoorden exporteren**. Het exportvenster wordt geopend.

3. Klik op **Selecteer het bestandstype**. Kies in het keuzemenu of u uw gegevens wilt exporteren in een JSON-formaat of een CSV-formaat. U kunt ook een wachtwoord invoeren om het geëxporteerde bestand te beveiligen.
   Vink het bijbehorende vakje aan als je ook gedeelde items wilt toevoegen.
4. Klik **Exporteren** in de linkeronderhoek van het exportvenster en sla het geëxporteerde bestand op uw apparaat op.

4. KENMERKEN EN FUNCTIONALITEITEN

In dit hoofdstuk worden alle kenmerken en functionaliteiten van Bitdefender Password Manager overlopen, met uitleg over hun nut en over hoe u ze zo efficiënt mogelijk kunt gebruiken.

4.1. Wachtwoorden handmatig opslaan

U kunt informatie zoals wachtwoorden, inloggegevens en andere gegevens, zoals creditcardgegevens of notities, op de volgende manier veilig handmatig in Bitdefender SecurePass opslaan:

1. Bitdefender SecurePass openen
2. In het **Mijn kluis** tab, druk op de **+Item toevoegen** knop.
3. Selecteer het itemtype dat je wilt toevoegen. (account, creditcard, identiteit of briefje).
4. Vul de verplichte velden in, afhankelijk van het geselecteerde item.
5. Nadat u alle benodigde gegevens hebt ingevuld, slaat u het item op om het aan uw SecurePass-kluis toe te voegen.

4.2. Wachtwoordgenerator

Bitdefender SecurePass bevat een functie voor het genereren van wachtwoorden die kan helpen bij het aanmaken van veilige wachtwoorden.

Om toegang te krijgen tot de wachtwoordgenerator en deze te gebruiken:

1. Open Bitdefender SecurePass en krijg toegang tot de **Wachtwoord genereren** tab aan de linkerkant van het scherm. Dit brengt u naar de wachtwoordgenerator die is geïntegreerd in SecurePass
2. Pas het wachtwoord dat u gaat genereren aan uw eigen behoeften en voorkeuren aan.
   - Wachtwoordlengte: versleep de schuifregelaar om een lengte tussen 8 en 32 tekens te bepalen.
   - Hoofdletters en kleine letters: Selecteer welke - of beide - soorten letters je wilt toevoegen voor het complexiteitsniveau van je wachtwoord.

- Getallen: Als u dit vakje aanvinkt, worden cijfers opgenomen in de tekenreeks die uw wachtwoord bevat.
- Speciale tekens: Voeg symbolen toe aan je wachtwoord om de complexiteit van het wachtwoord te vergroten.

> **Opmerking**
> Druk op de **Instellingen opslaan** knop voor SecurePass om ze te onthouden en altijd wachtwoorden te genereren op basis van de instellingen die je hebt opgeslagen.

3. Genereer een nieuw wachtwoord door op het ronde pijlpictogram te klikken dat zich onder het momenteel weergegeven wachtwoord bevindt. Elke klik genereert een nieuwe reeks tekens.
4. Als u tevreden bent met het gegenereerde wachtwoord, kunt u het naar uw klembord kopiëren of op de knop klikken **Account opslaan** knop om het in uw kluis op te slaan (door te koppelen aan andere accountgegevens).

> **Opmerking**
> Je kunt ook snel een wachtwoord genereren **rechtstreeks vanuit aanmeldingsformulieren** door te klikken op het Bitdefender SecurePass-pictogram in het wachtwoordveld van de aanmeldingspagina. Door erop te klikken, kunt u vervolgens kiezen voor de **Wachtwoord genereren** optie.

4.3. Controle van de wachtwoordsterkte

Bitdefender SecurePass biedt de mogelijkheid om de sterkte van opgeslagen wachtwoorden en gevoelige gegevens te evalueren. Dit is van essentieel belang bij het evalueren en beoordelen van mogelijke kwetsbaarheden in de privacy en beveiliging van uw gegevens.

Ga als volgt te werk om de sterke punten van opgeslagen wachtwoorden te controleren:

1. Open Bitdefender SecurePass en selecteer in het mailmenu de optie **Beveiligingsrapport** tab.
   Het tabblad Beveiligingsrapport is onderverdeeld in vier secties: geschonden, zwak, oud en dubbel.
2. Het aantal wachtwoorden dat in elk van de vier categorieën valt, wordt op het scherm weergegeven.

Als u de lijst met opgeslagen wachtwoorden doorloopt, wordt elk wachtwoord bovendien getagd met de categorie waaronder het zich bevindt.

Om de betekenis achter deze beveiligingsniveaus te begrijpen, vindt u hieronder enkele beknopte informatie over elk van deze niveaus:

- Wachtwoorden die zijn geschonden: Als een van uw inloggegevens deel heeft uitgemaakt van een datalek, worden deze vermeld onder de **doorbroken** sectie.

  > **Opmerking**
  > Om te controleren of een van uw wachtwoorden is gehackt en gelekt door datalekken, klikt u op de **Voer een beveiligingsscan uit** knop.

- Zwakke wachtwoorden: SecurePass identificeert en markeert **zwak** wachtwoorden die in uw kluis zijn opgeslagen op basis van een intern, lokaal draaiend algoritme dat onder andere naar verschillende criteria kijkt, zoals de lengte van het wachtwoord, het aantal tekens en het opnemen van cijfers of hoofdletters.
- Oude wachtwoorden: Wachtwoorden die langer dan zes maanden zijn opgeslagen en ongewijzigd zijn gebleven, worden gemarkeerd als **oud**.
- Dubbele wachtwoorden: Aangezien het gebruik van dezelfde wachtwoorden op meerdere platforms en accounts een groot veiligheidsrisico inhoudt, zal SecurePass wachtwoorden die op meer dan één plaats worden gebruikt, markeren als **duplicaat**.

4.4. Organisatie van de gegevens

Binnen Bitdefender SecurePass kunt u al uw opgeslagen items organiseren en dus eenvoudiger beheren.

Je kunt je items in specifieke mappen indelen voor eenvoudige toegang door deze stappen te volgen:

1. Open Bitdefender SecurePass en ga naar **Mijn kluis**. Tik hier op de **Folder toevoegen** knop.
2. Geef je map een naam en tik op **Creëren** knop.
   De nieuwe map verschijnt nu in je kluis.

Om items naar de aangemaakte map te verplaatsen:

1. Klik op een account dat je wilt verplaatsen en druk op **Bewerken** knop.
2. Druk op de locatie die wordt weergegeven naast **Item opslaan in** en selecteer de mapnaam in de keuzelijst.
3. Druk op de **Account opslaan** knop.

Het account wordt nu opgeslagen in de geselecteerde map.

4.5. Intelligente automatische aanvulling

Met Bitdefender SecurePass kunt u accountgegevens en -informatie automatisch invullen op alle online aanmeldingsformulieren.

> **Opmerking**
> Als webbrowserextensie zou de functie Automatisch aanvullen op Windows of MacOS naadloos moeten werken.

4.5.1. Automatisch aanvullen op Android

Om SecurePass op Android te configureren om Autofill te gebruiken:

1. Open de Bitdefender SecurePass-app op je Android-apparaat.
2. Tik op de **Meer** menuknop.
3. Tik bovenaan het scherm op **Instellingen**.
4. Tik op **Maak dit uw standaard wachtwoordbeheerder**
5. Schakel Bitdefender SecurePass in de lijst met services voor automatisch aanvullen in.

> **Opmerking**
> Je kunt ook naar de instellingen van je Android-apparaat gaan, in **Wachtwoorden en accounts** > **Service voor automatisch aanvullen** > schakel Bitdefender SecurePass in.
>
> Voor Android 11 of eerdere versies van het besturingssysteem zijn de instellingen: **Systeem** > **Taal en invoer** > **Geavanceerd**.

6. Tik **OK**.

Zodra deze configuratie is voltooid, verschijnt er telkens wanneer u op een aanmeldingsveld tikt een optie genaamd Bitdefender SecurePass op uw scherm. Je kunt erop tikken om de app te openen. Meld u aan bij SecurePass en uw inloggegevens worden automatisch ingevuld

4.5.2. Automatisch aanvullen op iOS

Om SecurePass op uw iOS-apparaat te configureren om Autofill te gebruiken:

1. Open het **Instelling** app op je iPhone of iPad en selecteer **Algemeen**.
2. Tik op **Automatisch aanvullen en wachtwoorden**. Zorg voor de optie **Wachtwoorden en wachtwoordsleutels automatisch invullen** of **Wachtwoorden automatisch invullen** - afhankelijk van de iOS-versie - is ingeschakeld.
3. In het **Formulier automatisch invullen** lijst, schakel de **Bitdefender SecurePass** applicatie.

Zodra deze configuratie is voltooid, verschijnt er telkens wanneer u op een aanmeldingsveld tikt een optie genaamd Bitdefender SecurePass op uw scherm. Je kunt erop tikken om de app te openen. Meld u aan bij SecurePass en uw inloggegevens worden automatisch ingevuld

4.5.3. Kaartgegevens automatisch invullen

SecurePass biedt een gemakkelijk toegankelijk pictogram voor het automatisch invullen van inloggegevens en wachtwoorden, maar de functie voor automatisch aanvullen van creditcardgegevens werkt anders:

1. Navigeer naar de betalings- of betaalpagina van de website waarop u uw opgeslagen creditcardgegevens wilt gebruiken.
2. Klik met de rechtermuisknop op een leeg gedeelte van de betaalpagina. Dit zal ertoe leiden dat het contextmenu op uw scherm verschijnt
3. Selecteer Bitdefender SecurePass in het menu door de muisaanwijzer op de optie te bewegen. Dit opent een submenu met meer opties
4. Kies de **Creditcardgegevens automatisch invullen**. Hiermee wordt een lijst weergegeven van alle creditcards die u in de SecurePass-kluis hebt opgeslagen
5. Selecteer de gewenste kaart.

Op deze manier vult SecurePass de velden van het betalingsformulier automatisch in met de gegevens van de creditcard die u hebt gekozen.

5. GEBRUIK ALS EEN 2FA-APPLICATIE

U kunt er altijd voor kiezen om Bitdefender SecurePass te gebruiken als een app voor tweefactorauthenticatie voor elke website of elk gewenst platform, en uw 2FA-codes naast uw wachtwoorden op de volgende manier te beheren:

1. Ga naar de beveiligingsinstellingen van de website of applicatie waar je de 2FA-functie wilt inschakelen. Meestal krijgt u tijdens het proces een QR-code of een verificatiecode te zien.
2. Start Bitdefender SecurePass en open het corresponderende account dat u wilt configureren voor 2FA-gebruik. Klik op de **Bewerken** knop.
3. Blader naar de onderkant van de accountinvoerpagina in SecurePass en druk op de **Twee-factor-authenticatie** optie.
4. Scan de QR-code of voer de code handmatig in.
   Zodra dit is gebeurd, bevestigt SecurePass de succesvolle configuratie van tweefactorauthenticatie.
5. Druk daarna op de nieuwe **Code bekijken** knop nu zichtbaar in de interface. Daar wordt een tijdgevoelige code weergegeven
6. Ga terug naar het account waar u de 2FA-functie hebt ingeschakeld en voer de code van Bitdefender SecurePass in om uw configuratie te verifiëren.

Na het voltooien van dit installatieproces drukt u op de **Account opslaan** knop in SecurePass om het proces te voltooien.

Voortaan wordt u, wanneer u inlogt op het platform waarvoor u de 2FA-functie hebt ingesteld, gevraagd om de 2FA-codes van SecurePass te gebruiken voor het betreffende account, wat een nieuwe beveiligingslaag biedt voor het betreffende account.

6. GEGEVENS DELEN

Bitdefender SecurePass biedt de mogelijkheid om gevoelige informatie, zoals inloggegevens, wachtwoorden of creditcardgegevens, veilig te delen.

Je kunt de deelfunctie gebruiken via links:

1. Kies een item dat is opgeslagen in je kluis.
   - In de browser:
     Ga naar je kluis en klik op het item dat je wilt delen. Klik aan de rechterkant op het menu met de drie puntjes en selecteer **Link delen**.
   - In de app:
     Ga naar je kluis en tik op het item dat je wilt delen. Tik op het linkpictogram en kies de **Genereer een link om te delen** optie.
2. Maak de link Delen door het volgende op te geven:
   - De vervaldatum van de link.
   - De gebruikslimiet.
   - Of de link wel of niet met een wachtwoord moet worden beveiligd.
3. Eenmaal gegenereerd, kopieert u de gegenereerde link en stuurt u deze naar de beoogde ontvanger.

6.1. Delen met groepen

Er worden groepen gemaakt om het delen van gegevens nog eenvoudiger te maken. U kunt binnen Bitdefender SecurePass verschillende groepen aanmaken met andere gebruikers om gevoelige gegevens veilig te delen

1. Een groep aanmaken:
   - Ga naar **Groepen** en druk op de **Een groep aanmaken** knop op het tabblad Groepen.
   - Stel een groepsnaam in en druk vervolgens op **Een groep aanmaken** knop.
2. Items aan groepen toevoegen:
   - In de browser:

Ga naar je kluis en klik op het item dat je wilt delen. Klik op het menu met de drie puntjes aan de rechterkant van het item en kies **Aan groep toevoegen**.

- In de app:
  Ga naar je kluis en klik op het item dat je wilt delen. Kies de **Deel met de groep** optie.

Selecteer de groep waarmee je het item wilt delen.

3. Stel de toegangsrechten (lezen, schrijven, verlenen) in op basis van de mate van controle die je groepsleden wilt geven.
4. Druk op **Opslaan**, dan **Klaar**.

Jij en groepsleden kunnen gedeelde items bekijken in de sectie van de groep.

6.2. Groepen beheren

In het **Groepen** in het gedeelte van Bitdefender SecurePass kunt u alle aangemaakte groepen bekijken en beheren op basis van uw behoeften:

- Groepen hernoemen.
- Leden bewerken. (nieuwe leden uitnodigen, rechten toekennen aan specifieke leden, beheer- of deelrechten verlenen en bestaande leden verwijderen)
- Groepen verlaten.
- Groepen verwijderen.

7. ACCOUNT VERGRENDELEN

Bitdefender SecurePass wordt geleverd met een **Account vergrendelen** functie die uw account onmiddellijk vergrendelt en alle actieve sessies beëindigt op alle apparaten die er toegang toe hebben. Deze functie is vooral handig wanneer er vermoedens van ongeoorloofde toegang ontstaan

Om uw SecurePass-account te vergrendelen:

1. Open Bitdefender SecurePass.
2. Eenmaal in SecurePass:
   - In de browser:
     Klik op **Instellingen** in de rechterbovenhoek van de pagina.
   - In de mobiele app:
     Tik op de **Beveilig me** menuknop.
3. Druk op de **Account vergrendelen** knop om direct uit te loggen van alle apparaten en lopende sessies te beëindigen.

8. VEELGESTELDE VRAGEN

Sommige veelgestelde vragen over Bitdefender Password Manager komen vaak terug. Wij hebben de antwoorden! Hier vindt u meer informatie over uw Bitdefender-account, het importeren van wachtwoorden, protocollen voor gegevensbeveiliging en andere onderwerpen die belangrijk zijn voor onze klanten.

Algemene vragen over Bitdefender Password Manager

Wat gebeurt er wanneer Bitdefender Password Manager vervalt?

Wanneer uw abonnement op Bitdefender Password Manager vervalt en niet langer actief is, hebt u maximaal 90 dagen de tijd om uw wachtwoorden te exporteren. De wachtwoorden worden nog 30 dagen in een back-up bewaard. Gedurende deze 90 dagen kunt u alleen uw gegevens exporteren. U kunt Bitdefender Password Manager niet meer gebruiken. De functie voor automatisch invullen werkt niet meer, evenmin als de mogelijkheid om wachtwoorden te genereren.

Aan het einde van de 90 dagen respijtperiode hebt u 30 dagen extra de tijd om contact op te nemen met de ondersteuning van Bitdefender en een verzoek in te dienen om uw wachtwoorden terug te zetten naar de live database. U zult dan uw wachtwoorden kunnen exporteren vanuit Bitdefender Password Manager.

Uw gegevens worden alleen in de live database bewaard tot het einde van de dag dat ze op verzoek werden hersteld. Om middernacht wordt de database gewist - en als u de extra periode van 30 dagen nog niet hebt overschreden, kunnen de wachtwoorden opnieuw worden hersteld vanuit de back-up. Op verzoek van de gebruiker kunnen de ruwe databasegegevens uit de back-up worden verstrekt, maar de database is gecodeerd en de informatie is niet toegankelijk.

Wat is een hoofdwachtwoord en waarom moet ik het onthouden?

Het hoofdwachtwoord is de sleutel die de deur opent naar alle wachtwoorden die in uw Bitdefender Password Manager-account zijn opgeslagen. Het hoofdwachtwoord moet ten minste 8 tekens lang zijn. Maak dus een sterk hoofdwachtwoord, onthoud het en deel het nooit met iemand. Om een sterk hoofdwachtwoord te maken, raden we u aan

een combinatie te gebruiken van hoofdletters en kleine letters, cijfers en speciale tekens (zoals #, $, of @).

Waarom slaan jullie mijn hoofdwachtwoord niet op, en wat gebeurt er als ik het vergeet?

De reden waarom we uw hoofdwachtwoord niet opslaan op onze servers is dat alleen u toegang heeft tot uw account. Het is de meest veilige manier. Als Bitdefender Password Manager uw hoofdwachtwoord niet herkent, controleer dan of u het correct typt en of de Caps Lock-toets niet actief is op het toetsenbord.

Als u het hoofdwachtwoord vergeet, kunt u altijd de Herstelsleutel gebruiken om Password Manager te ontgrendelen. Tijdens het aanmeldingsproces biedt Bitdefender Password Manager een **herstelsleutel** die kan worden gebruikt om weer toegang te krijgen tot de account zonder uw gegevens te verliezen.

Wat is de offlinemodus?

offlinemodus wordt automatisch geactiveerd wanneer de internetverbinding wegvalt tijdens het gebruik van Bitdefender SecurePass. Als u al bent aangemeld en uw hoofdwachtwoord hebt ingevoerd, kunt u in de modus Offline toegang krijgen tot uw wachtwoorden wanneer een internetverbinding buiten bereik is.

Hoe kan ik de installatie van Bitdefender Password Manager ongedaan maken?

Bitdefender Password Manager de-installeren:

- Op Windows en macOS:
  Verwijder de Password Manager-extensie uit uw webbrowser. Klik met de rechtermuisknop op het Bitdefender-pictogram en selecteer "Verwijderen".
- Android:
  Tik en houd de Password Manager-app ingedrukt en sleep deze naar de bovenkant van het scherm waar "Verwijderen" staat.
- Op iOS en iPadOS:
  Tik op de app Password Manager en houd deze ingedrukt totdat alle apps op uw scherm beginnen te wiebelen, tik vervolgens op de "X" linksboven het Bitdefender-pictogram.

Veiligheidsvragen over Bitdefender Password Manager

Kunnen medewerkers van Bitdefender mijn wachtwoorden zien?

Absoluut niet. Uw privacy is onze hoogste prioriteit. Dit is de belangrijkste reden waarom we uw hoofdwachtwoord niet opslaan op onze gegevensservers: zodat niemand toegang heeft tot uw account, zelfs niet de medewerkers van het bedrijf. Elk wachtwoord en account zijn sterk versleuteld met het sterkste algoritme voor gegevensbeveiliging, en de code die we zien ziet er gewoon uit als een willekeurige reeks cijfers en letters die door elkaar zijn gegooid.

Wat zou er gebeuren als de servers van Password Manager worden gehackt?

Elk wachtwoord wordt lokaal op uw apparaat gecodeerd voordat het in de buurt van onze servers komt, dus als hackers in ons systeem zouden inbreken, zouden ze alleen pagina's met willekeurige letters en cijfers krijgen zonder uw sleutel om ze te decoderen. Dit betekent dat u en uw accountgegevens bij ons altijd veilig zijn.

9. HULP VRAGEN

9.1. Hulp vragen

Bitdefender biedt zijn klanten een ongeëvenaard niveau van snelle en nauwkeurige ondersteuning. Als u een probleem ondervindt of een vraag hebt over uw Bitdefender-product, kunt u verschillende online bronnen gebruiken om een oplossing of een antwoord te vinden. Tegelijkertijd kunt u contact opnemen met het klantenserviceteam van Bitdefender. Onze ondersteuningsmedewerkers zullen uw vragen tijdig beantwoorden en u de hulp bieden die u nodig hebt.

9.2. Online bronnen

Er zijn meerdere online informatiebronnen beschikbaar om u te helpen bij het oplossen van problemen en vragen met betrekking tot Bitdefender.

- Bitdefender Support Center:
  https://www.bitdefender.nl/consumer/support/
- De Community van Bitdefender-experts:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

U kunt ook uw favoriete zoekmachine gebruiken om meer informatie te zoeken over computerbeveiliging, de Bitdefender-producten en het bedrijf.

9.2.1. Bitdefender Support Center

Het Bitdefender Support Center is een online opslagplaats van informatie over Bitdefender-producten. Hier worden rapporten bijgehouden in een gemakkelijk toegankelijk formaat over de doorlopende technische ondersteuning en activiteiten voor foutoplossingen van de ondersteunings- en ontwikkelingsteams van Bitdefender. Daarnaast vindt u hier ook meer algemene artikels over dreigingspreventie, het beheer van Bitdefender-oplossingen met gedetailleerde uitleg en talrijke andere artikels.

De Bitdefender Support Center is toegankelijk voor het publiek en kan vrij worden doorzocht. De uitgebreide informatie die de database bevat is nog

een middel om BitDefender-klanten de technische kennis en het inzicht te bieden die ze nodig hebben. Alle geldige aanvragen voor informatie of foutrapporten die van BitDefender-klanten komen, vinden uiteindelijk hun weg naar de Bitdefender Support Center als rapporten over het oplossen van problemen, tips om een probleem te omzeilen of informatieve artikels om de helpbestanden van het product aan te vullen.

Het Bitdefender Support Center is te allen tijde beschikbaar op het volgende adres: https://www.bitdefender.nl/consumer/support/.

9.2.2. De Community van Bitdefender-experts

De Community van Experts is een omgeving waar gebruikers, enthousiastelingen en fans van Bitdefender aan kunnen deelnemen, waar ze ideeën kunnen uitwisselen, elkaar kunnen ondersteunen en hun kennis en oplossingen kunnen delen. Het is ook een plaats voor brainstorming en een bron van waardevolle feedback aan onze ontwikkelingsteams. De leden van de gemeenschap zijn ervaren Bitdefender-gebruikers die in hun eigen tijd graag anderen helpen. Met hun enorme bijdrage en oprechte vrijwillige inspanningen hebben we een kennisbank gecreëerd waar gebruikers antwoorden en begeleiding kunnen vinden, maar met dat menselijke tintje.

Hier vindt u zinvolle gesprekken met mensen die Bitdefender gebruiken op hun apparaten. De gemeenschap biedt een echte band met onze leden en laat uw stem horen. Het is een plek waar u wordt aangemoedigd om deel te nemen in de wetenschap dat uw mening en inbreng worden gerespecteerd en gekoesterd. Als gewaardeerde provider streven we ernaar een ongeëvenaard niveau van snelle, accurate ondersteuning te bieden en willen we onze gebruikers dichter bij ons brengen. Wij hebben onze gemeenschap met dit doel voor ogen ontworpen.

U vindt de website van onze Community van experts hier:

https://community.bitdefender.com/en/

9.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia heeft alle informatie die u nodig hebt over de nieuwste cyberdreigingen. Dit is de plaats waar Bitdefender-experts tips en trucs delen over hoe u beschermd kunt blijven tegen hackers, datalekken, identiteitsdiefstal en pogingen tot sociale imitatie.

De webpagina van Bitdefender Cyberpedia vindt u hier:

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

9.3. Contactinformatie

Efficiënte communicatie is de sleutel tot succes. Sinds 2001 heeft BITDEFENDER een onberispelijke reputatie opgebouwd door voortdurend te streven naar een betere communicatie om de verwachtingen van onze klanten en partners telkens te overtreffen. Aarzel daarom niet om rechtstreeks contact met ons op te nemen als u iets wilt vragen, via onze Bitdefender Support Center.

https://www.bitdefender.nl/consumer/support/

9.3.1. Lokale verdelers

De lokale BitDefender-verdelers zijn altijd paraat om te reageren op aanvragen met betrekking tot hun bedrijfsgebied, zowel op commercieel als algemeen vlak.

Om een Bitdefender-verdeler te vinden in uw land:

1. Ga naar https://www.bitdefender.com/partners/partner-locator.html.
2. Kies uw land en stad met de overeenkomstige opties.

WOORDENLIJST

Activeringscode

Is een unieke sleutel die u in de handel kunt kopen en die gebruikt wordt om een specifiek product of een dienst te activeren. Met een activeringscode kan een geldig abonnement voor een bepaalde periode en een bepaald aantal toestellen geactiveerd worden en kunt u ook gebruiken om het abonnement te verlengen, op voorwaarde dat het voor hetzelfde product of dezelfde dienst is.

ActiveX

ActiveX is een model voor het schrijven van programma's zodat andere programma's en het besturingssysteem ze kunnen oproepen. De ActiveX-technologie wordt gebruikt bij Microsoft Internet Explorer om interactieve Webpagina's te maken die eruitzien en zich gedragen als computerprogramma's in plaats van statische pagina's. Met ActiveX kunnen gebruikers vragen stellen of beantwoorden, drukknoppen gebruiken en op andere manieren interactief omgaan met de Webpagina. ActiveX-besturingselementen zijn vaak geschreven met de hulp van Visual Basic. ActiveX is berucht door een compleet gebrek aan beveiligingscontroles; computerbeveiligingsexperts raden het gebruik ervan via het internet sterk af.

Advanced persistent threat

Geavanceerde aanhoudende dreiging (Advanced Persistent Threat - APT) maakt misbruik van kwetsbare plekken in systemen om belangrijke informatie te stelen en aan de bron te leveren. Grote groepen, zoals organisaties, bedrijven of overheden zijn doelgroepen voor deze bedreiging. Het doel van een advanced persistent threat is heel lang onopgemerkt te blijven en belangrijke informatie in te kijken en te verzamelen, zonder de toestellen te beschadigen. De methode die gebruikt wordt om de bedreiging in het netwerk te brengen verloopt via een pdf-bestand of een Office-document dat er onschuldig uitziet, zoadat elke gebruiker de bestanden kan openen.

Adware

Adware wordt vaak gecombineerd met een hosttoepassing die gratis wordt aangeboden op voorwaarde dat de gebruiker akkoord gaat met het uitvoeren van de adware. Omdat adware-toepassingen doorgaans

worden geïnstalleerd nadat de gebruiker een licentieovereenkomst die het doel van de toepassing vermeldt heeft geaccepteerd, wordt er geen inbreuk gepleegd. Pop-upadvertenties kunnen echter irritant worden en in sommige gevallen de systeemprestaties negatief beïnvloeden. De gegevens die door sommige van deze toepassingen worden verzameld, kunnen bovendien privacy-problemen veroorzaken voor gebruikers die niet volledig op de hoogte waren van de voorwaarden van de licentieovereenkomst.

Archive

Een schijf, tape, of map die bestanden bevat waarvan een back-up werd gemaakt.

Een bestand dat één of meer bestanden bevat in een gecomprimeerd formaat.

Backdoor

Een gat in de beveiliging van een systeem, dat opzettelijk werd achtergelaten door ontwikkelaars of beheerders. De motivatie voor dergelijke gaten is niet altijd boosaardig. Sommige besturingssystemen worden bijvoorbeeld geleverd met bevoegde accounts die bedoeld zijn voor gebruik door technici voor service ter plaatse of onderhoudsprogrammeurs van de leverancier.

Boot sector

Een sector aan het begin van elke schijf die de architectuur van de schijf identificeert (sectorgrootte, clustergrootte, enz.) Bij opstartschijven bevat de opstartsector ook een programma dat het besturingssysteem laadt.

Boot virus

Een bedreiging die de opstartsector van een vaste schijf of een diskette infecteert. Wanneer u probeert op te starten vanaf een diskette die geïnfecteerd is met een opstartsectorvirus, zal de bedreiging actief worden in het geheugen. Wanneer u vanaf dat ogenblik uw systeem opstart, zal de bedreigingen telkens in het geheugen geactiveerd zijn.

Botnet

Het woord "botnet" is samengesteld uit de woorden "robot" en "netwerk". Botnets zijn apparaten die met het internet verbonden zijn en met bedreigingen geïnfecteerd zijn en kunnen gebruikt worden om spammail te verzenden, data te stelen, kwetsbare apparaten van op afstand

te controleren of om spyware, ransomware en andere schadelijke bedreigingen te verspreiden. Het doel ervan is zoveel mogelijk apparaten te infecteren, bijvoorbeeld pc's, servers, mobiele of IoT-apparaten die eigendom zijn van grote bedrijven of sectoren.

Browser

De korte naam voor Webbrowser, een softwaretoepassing die wordt gebruikt op Webpagina's te zoeken en weer te geven. Populaire browsers omvatten Microsoft Internet Explorer, Mozilla Firefox en Google Chrome. Dit zijn grafische browsers. Dit betekent dat ze zowel grafische beelden als tekst kunnen weergeven. Bovendien kunnen de meeste moderne browsers ook multimedia-informatie voorstellen met geluid en video, hoewel voor sommige formaten plug-ins vereist zijn.

Brute Force-aanval

Aanval via raden van wachtwoord, gebruikt om in te breken in een computersysteem door mogelijke wachtwoordcombinaties in te geven, meestal te beginnen met het meest eenvoudig te raden wachtwoord.

Opdrachtregel

In een opdrachtregelinterface typt de gebruiker opdrachten in opdrachttaal rechtstreeks op het scherm in de ruimte die hiervoor wordt geboden.

Cookies

Binnen de Internetindustrie worden cookies beschreven als kleine programma's die informatie bevatten over individuele computers, die door adverteerders wordt geanalyseerd en gebruikt om uw on line interesse en smaak te volgen. De cookietechnologie wordt in dit kader nog steeds verder ontwikkeld met het doel reclameberichten rechtstreeks te richten op de interesses die u hebt meegedeeld. Dit is voor veel mensen een mes dat aan twee kanten snijdt. Aan de ene kant is het efficiënt en relevant aangezien u alleen reclames ontvangt voor zaken waarvoor u interesse hebt. Aan de andere kant betekent het ook dat elke plaats die u bezoekt en alles wat u aanklikt wordt "opgespoord" en "gevolgd". Het is dan ook te begrijpen dat er heel wat wordt gedebatteerd over privacy. Bovendien zijn veel mensen verontwaardigd omdat ze het gevoel hebben dat ze als een "SKU-nummer" worden beschouwd (u weet wel, de barcode op de verpakkingen die bij de kassa van het warenhuis wordt gescand). Hoewel dit standpunt misschien nogal extreem is, is het vaak een bijzonder nauwkeurige omschrijving.

Cyberpesten

Wanneer collega's of onbekenden met opzet onrechtmatige daden stellen tegenover kinderen, met de bedoeling om fysiek te kwetsen. Om emotionele schade te berokkenen, sturen de daders gemene berichten of onflatteuze foto's om hun slachtoffers af te zonderen van anderen of gefrustreerd te doen voelen.

Woordenboekaanval

Aanval via raden van wachtwoord, gebruikt om in te breken in een computersysteem door een combinatie van veel voorkomende woorden in te geven om zo mogelijke wachtwoorden te genereren. Dezelfde methode wordt gebruikt om decryptiesleutels van versleutelde berichten of documenten te raden. Woordenboekaanvallen slagen in hun opzet omdat veel mensen korte wachtwoorden gebruiken die uit slechts één woord bestaan en die makkelijk te raden zijn.

Schijfstation

Dit is een apparaat dat gegevens leest van en schrijft naar een schijf. Een harde-schijfstation leest en schrijft harde schijven. Een diskettestation opent diskettes. Schijfstations kunnen intern (binnen de behuizing van een computer) of extern zijn (in een afzonderlijke behuizing die op de computer wordt aangesloten).

Download

Om gegevens (meestal een volledig bestand) te kopiëren van een hoofdbron naar een randapparaat. De term wordt vaak gebruikt om het proces te beschrijven waarbij een bestand van een on line-service wordt gekopieerd naar de eigen computer. Downloaden kan ook verwijzen naar het kopiëren van een bestand van een netwerkbestandsserver naar een computer in het netwerk.

E-mail

Elektronische post. Een dienst die berichten naar computers verzendt via lokale of globale netwerken.

Gebeurtenissen

Een actie of gebeurtenis die door een programma wordt gedetecteerd. Gebeurtenissen kunnen gebruikersacties zijn, zoals het klikken met de muis of het indrukken van een toets, of systeemgebeurtenissen, zoals een tekort aan geheugen.

Exploits

Een manier om misbruik te maken van verschillende bugs of kwetsbaarheden in een computer (software of hardware). Zo kunnen hackers de controle over computers of over netwerken in handen krijgen.

Vals positief

Doet zich voor wanneer een scanner een bestand ten onrechte beschouwt als geïnfecteerd.

Bestandsextensie

Het gedeelte van een bestandsnaam achter de punt, waarmee het gegevenstype dat in het bestand is opgeslagen wordt aangeduid. Heel wat besturingssystemen, zoals Unix, VMS en MS-DOS, maken gebruik van bestandsextensies. Ze gebruiken doorgaans één tot drie letters (sommige betreurenswaardige oude besturingssystemen ondersteunen niet meer dan drie letters). Voorbeelden hiervan zijn "c" voor C-broncode, "ps" voor PostScript, "txt" voor tekst zonder opmaak.

Heuristisch

Een methode voor het identificeren van nieuwe bedreigingen op basis van regels. Deze scanmethode is niet gebaseerd op een specifieke informatie-database voor bedreigingen. Het voordeel van de heuristische scan is dat hij zich niet laat misleiden door een nieuwe variant van een bestaande bedreiging. Dit type kan echter af en toe een verdachte code rapporteren in normale programma's, zodat de zogenoemde "valse positieve" rapporten worden gegenereerd.

Honeypot

Een afleiding in uw computersysteem dat hackers aantrekt om te onderzoeken hoe ze te werk gaan en de afwijkende methodes die ze gebruiken om systeeminformatie te verzamelen, te identificeren. Bedrijven zijn steeds meer geïnteresseerd om honingpotten te implementeren en te gebruiken om hun algemene beveiligingsstatus te verbeteren.

IP

Internet Protocol - Een routeerbaar protocol in de TCP/OP-protocolreeks die verantwoordelijk is voor de IP-adressering, routing en de fragmentatie en defragmentatie van IP-pakketten.

Java applet

Een Java-programma dat is ontwikkeld om alleen op een webpagina te worden uitgevoerd. Om een applet op een webpagina te gebruiken, zou u de naam van het applet opgeven en de grootte (lengte en breedte in pixels) die het applet kan gebruiken. Wanneer de webpagina wordt geopend, downloadt de browser het applet van een server en voert hij het uit op de computer van de gebruiker (de client). Applets onderscheiden zich van toepassingen omdat ze worden beheerd door een streng beveiligingsprotocol.

Zelfs wanneer applets op de client worden uitgevoerd kunnen ze, bijvoorbeeld, geen gegevens lezen van of schrijven naar de computer van de client. Bovendien worden applets verder beperkt zodat ze alleen gegevens kunnen lezen van en schrijven naar hetzelfde domein waarvan ze worden bediend.

Keylogger

Een keylogger is een toepassing die alles wat u typt, logt. Keyloggers zijn in wezen niet kwaadaardig. Ze kunnen worden gebruikt voor rechtmatige doeleinden, zoals het bewaken van de activiteiten van werknemers of kinderen. Ze worden echter steeds meer gebruikt door cybercriminele voor boosaardige doeleinden (bijv. voor het verzamelen van persoonlijke gegevens, zoals aanmeldingsgegevens en nummer van de sociale zekerheid).

Macro virus

Een type computerbedreiging die is gecodeerd als een macro die in een document is ingesloten. Talrijke toepassingen, zoals Microsoft Word en Excel, ondersteunen krachtige macrotalen. Met deze toepassingen kan u een macro in een document insluiten, en die macro telkens laten uitvoeren wanneer het document wordt geopend.

Mail client

Een e-mailclient is een toepassing waarmee u e-mail kunt verzenden en ontvangen.

Geheugen

Interne opslaggebieden in de computer. De term geheugen staat voor gegevensopslag die in de vorm van chips wordt geleverd. Het woord opslag wordt gebruikt voor geheugen dat aanwezig is op tapes of schijven. Elke computer wordt geleverd met een bepaalde hoeveelheid fysiek geheugen, dat meestal het hoofdgeheugen of RAM wordt genoemd.

Niet-heuristisch

Deze scanmethode is gebaseerd op een specifieke informatie-database voor bedreigingen. Het voordeel van de niet-heuristische scan is dat deze zich niet laat misleiden door iets dat kan lijken op een bedreiging en geen vals alarm genereert.

Online predatoren

Personen die minderjarigen of adolescenten met opzet willen betrekken in gesprekken, om hen zo te betrekken in illegale seksuele activiteiten. Sociale netwerken zijn de ideale plaats waar kwetsbare kinderen gemakkelijk kunnen worden verleid om seksuele activiteiten uit te voeren, online of tijdens fysieke ontmoetingen.

Ingepakte programma's

Een bestand in een gecomprimeerd formaat. Talrijke besturingssystemen en toepassingen beschikken over opdrachten waarmee u bestanden kunt inpakken, zodat ze minder geheugen in beslag nemen. Veronderstel bijvoorbeeld dat u een tekstbestand hebt dat tien opeenvolgende spatietekens bevat. Normaal zou dit tien bytes opslagruimte vereisen.

Een programma dat bestanden inpakt kan echter de spatietekens vervangen door een speciaal spatiereeks-teken, gevolgd door het aantal spaties dat wordt vervangen. In dit geval hebben de tien spaties slechts twee bytes nodig. Dit is slechts één inpaktechniek, maar er zijn er veel meer.

Pad

De exacte weg naar een bestand op een computer. Deze weg wordt doorgaans beschreven door middel van het hiërarchische bestandssysteem van boven naar beneden.

De route tussen twee willekeurige punten, zoals het communicatiekanaal tussen twee computers.

Phishing

Het onder valse voorwendselen verzenden van een e-mail aan een gebruiker, waarbij de indruk wordt gewekt dat het bericht afkomstig is van een bestaande onderneming, in een poging de gebruiker persoonlijke gegevens te ontfutselen die zullen worden gebruikt voor identiteitsroof. In het e-mailbericht wordt de gebruiker doorverwezen naar een website waar persoonlijke gegevens kunnen worden bijgewerkt,

zoals wachtwoorden en creditcard-, sofi- en bankrekeningnummers, die reeds in het bezit zijn van de rechtmatige organisatie. De website is echter nep en alleen opgezet om de gebruikersgegevens te stelen.

Foton

Photon is een vernieuwende, niet opdringerige Bitdefender technologie, ontworpen om de invloed van uw beveiligingsoplossing op de prestaties te beperken. Door de activiteit van uw pc's op de achtergrond te bewaken, maakt het gebruikspatronen die helpen opstart- en scanprocessen te optimaliseren.

Polymorf virus

Een bedreiging die zijn vorm wijzigt bij elk bestand dat het infecteert. Aangezien ze geen consequent binair patroon hebben, zijn dergelijke bedreigingen moeilijk te identificeren.

Poort

Een interface op een computer waarop u een apparaat kan aansluiten. PC’s hebben verschillende types poorten. Intern zijn er verschillende poorten voor het aansluiten van schijfstations, beeldschermen en toetsenborden. Extern beschikken PC’s over poorten voor het aansluiten van modems, printers, muizen en andere randapparatuur.

Bij TCP/IP- en UDP-netwerken, zijn ze een eindpunt voor een logische verbinding. Het poortnummer duidt aan over welk type poort het gaat. Poort 80 wordt bijvoorbeeld gebruikt voor HTTP-verkeer.

Ransomware

Ransomware is kwaadaardige software waarmee criminelen proberen geld af te persen van gebruikers, door hun systemen ontoegankelijk te maken totdat er losgeld is betaald. Enkele van de vele varianten van ransomware voor persoonlijke computersystemen zijn CryptoLocker, CryptoWall en TeslaWall.

De infectie kan verspreid worden door spam-e-mail te openen, e-mailbijlagen te openen of toepassingen te installeren zonder dat de gebruiker weet wat er op zijn systeem gaande is. Dagelijkse gebruikers en bedrijven vormen een doelwit voor ransomwarehackers.

Rapportbestand

Een bestand dat de acties weergeeft die zich hebben voorgedaan. BitDefender houdt een rapportbestand bij met het gescande pad,

het aantal gescande mappen, archieven en bestanden, en het aantal gevonden geïnfecteerde en verdachte bestanden.

Rootkit

Een rootkit is een verzameling softwareprogramma's die op beheerdersniveau toegang biedt tot een systeem. Deze term werd voor het eerst gebruikt voor Unix-besturingssystemen en verwees naar opnieuw gecompileerde hulpprogramma's die beheerdersrechten gaven aan indringers, zodat ze hun aanwezigheid konden verbergen en onzichtbaar bleven voor de echte systeembeheerders.

De belangrijkste functie van rootkits is het verbergen van processen, bestanden, logins en logbestanden. Rootkits die de hiervoor benodigde software bevatten, kunnen ook gegevens onderscheppen van terminals, netwerkverbindingen of randapparaten.

Rootkits zijn in wezen niet kwaadaardig. Systemen en zelfs sommige toepassingen verbergen kritieke bestanden met de hulp van rootkits. Ze worden echter het vaakst gebruikt om bedreigingen of de aanwezigheid van een indringer op het systeem te verbergen. In combinatie met bedreigingen, vormen rootkits een ernstige bedreiging voor de integriteit en beveiliging van een systeem. Ze kunnen het verkeer controleren, achterpoortjes in het systeem maken, bestanden en logboeken wijzigen en detectie vermijden.

Script

Script, een andere term voor een macro of batchbestand, is een lijst opdrachten die kunnen worden uitgevoerd zonder tussenkomst van de gebruiker.

Spam

Elektronische junkmail of berichten van junknieuwsgroepen. Algemeen bekend als ongewenste e-mail.

Spyware

Elke software die heimelijk gebruikersgegevens verzamelt via de internetverbinding van de gebruikers zonder dat hij/zij zich hiervan bewust is, doorgaans voor reclamedoeleinden. Spywaretoepassingen worden doorgaans gebundeld als een verborgen onderdeel van freeware- of sharewareprogramma's die kunnen worden gedownload van het internet. We moeten echter wel vermelden dat de meeste shareware- en freewaretoepassingen geen spyware bevatten. Zodra de spyware is

geïnstalleerd, worden de activiteiten van de gebruiker op het internet gevolgd en wordt deze informatie op de achtergrond naar iemand anders doorgestuurd. Spyware kan ook informatie verzamelen over e-mailadressen en zelfs wachtwoorden en creditcardnummers.

Spyware is vergelijkbaar met een Trojaans paard omdat gebruikers ook in dat geval het product onbewust installeren wanneer ze een ander programma installeren. Een veel voorkomende manier waarbij men het slachtoffer wordt van spyware is bepaalde P2P-programma's voor bestandsuitwisseling te downloaden.

Naast het feit dat deze methode onethisch is en een inbreuk op de privacy van de gebruiker betekent, steelt spyware van de gebruiker door de geheugenbronnen van de computer te gebruiken en bandbreedte te verbruiken wanneer de informatie naar de thuisbasis van de spyware wordt verzonden via de internetverbinding van de gebruiker. Aangezien spyware geheugen- en systeemgeheugen gebruikt, kunnen de toepassingen die op de achtergrond worden uitgevoerd leiden tot systeemfouten of een algemene systeeminstabiliteit.

Startup items

Elk bestand in deze map wordt geopend wanneer de computer wordt gestart. Een opstartitem kan bijvoorbeeld een opstartscherm zijn, een geluidsbestand dat moet worden afgespeeld wanneer de computer voor de eerste maal opstart, een herinneringsagenda of apps. In normale omstandigheden wordt een alias van een bestand in deze map geplaatst, en niet het bestand zelf.

Abonnement

Koopovereenkomst die u het recht heeft om een specifiek(e) product of dienst op een specifiek aantal toestellen en voor een bepaalde tijd te gebruiken. Een vervallen abonnement kan automatisch worden verlengd met gebruik van de informatie van de gebruiker tijdens de eerste aankoop.

Systeemvak

Het systeemvak, dat met Windows 95 werd ingevoerd, bevindt zich in de taakbalk van Windows (doorgaans onderaan naast de klok) en bevat miniatuurpictogrammen die systeemfuncties zoals fax, printer, modem, volume en meer, gemakkelijk toegankelijk maken. Dubbelklik of klik met de rechtermuisknop op een pictogram om de details en de besturingselementen te bekijken en te openen.

TCP/IP

Transmission Control Protocol/Internet Protocol - Een reeks netwerkprotocollen, wijdverspreid gebruikt op het internet, die communicatie bieden tussen onderling verbonden computernetwerken met verschillende hardware-architecturen en diverse besturingssystemen. TCP/IP bevat standaarden voor de manier waarop computers communiceren en regels voor het aansluiten van netwerken en het routeren van het verkeer.

Dreiging

Een programma of een deel van een code die op uw computer wordt geladen zonder uw medeweten en tegen uw wil wordt uitgevoerd. De meeste bedreigingen kunnen zichzelf ook dupliceren. Alle computerbedreigingen zijn door de mens gemaakt. Een eenvoudige bedreiging die zichzelf steeds opnieuw kan dupliceren is relatief eenvoudig te maken. Zelfs een dergelijke eenvoudige bedreiging is gevaarlijk aangezien het snel al het beschikbare geheugen zal opgebruiken en het systeem zal blokkeren. Een nog gevaarlijker type is een bedreiging die in staat is zichzelf te verzenden via netwerken en beveiligingssystemen te omzeilen.

informatie-updates van dreigingen

Het binaire patroon van een bedreiging, gebruikt door de beveiligingsoplossing om de bedreiging te detecteren en te verwijderen.

Trojaans paard

Een destructief programma dat zich voordoet als een goedaardige toepassing. In tegenstelling tot kwaadaardige softwareprogramma's en wormen, vermenigvuldigen Trojaanse paarden zich niet, maar ze kunnen even vernietigend zijn. Een van de meest verraderlijke bedreigingstypes van de Trojaanse paarden is een programma dat beweert dat het uw computer kan bevrijden van bedreigingen, maar dat in werkelijkheid bedreigingen op uw computer installeert.

De naam komt uit een verhaal uit de Ilias van Homerus. De Grieken schonken hun vijanden, de Trojanen, een reusachtig houten paard, zogenaamd als vredesgebaar. Maar nadat de Trojanen het paard binnen de stadsmuren hadden gesleept, kwamen de Griekse soldaten uit de holle romp van het paard tevoorschijn en openden ze de poorten van de stad, zodat hun landgenoten Troje konden binnendringen en veroveren.

Update

Een nieuwe versie van een software- of hardwareproduct, dat werd ontwikkeld om een oudere versie van hetzelfde product te vervangen. Daarnaast zullen de installatieroutines voor updates vaak controleren of er reeds een oudere versie van het product op uw computer is geïnstalleerd. Is dat niet het geval, dan kunt u de update niet installeren.

Bitdefender heeft zijn eigen updatefunctie waarmee u handmatig kunt controleren op updates of die het product automatisch kan updaten.

Virtueel privénetwerk (VPN)

Dit is een technologie die een tijdelijke en versleutelde rechtstreekse verbinding met een zeker netwerk over een minder beveiligd netwerk mogelijk maakt. Op die manier is het verzenden en ontvangen van data veilig en versleuteld, zodat ze moeilijk te vangen is door spionnen. Een bewijs van veiligheid is de authentificatie, die enkel mogelijk is via een gebruikersnaam en wachtwoord.

Worm

Een programma dat zich verspreidt via een netwerk en zichzelf ondertussen reproduceert. Dit type kan zich niet vasthechten aan andere programma's.