GEBRUIKSAANWIJZING

Bitdefender CONSUMER SOLUTIONS

Password Manager

Bitdefender Password Manager

Handleiding

Publicatiedatum 09/06/2023

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 Password Manager 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 Password Manager en het installatieproces.

Kenmerken en functionaliteiten (pagina 19)

Leer hoe u Bitdefender Password Manager en al zijn functies gebruikt.

Hulp vragen (pagina 30)

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 PASSWORD MANAGER

Bitdefender Password Manager 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 Password Manager 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. Beveiliging en hoe het werkt

Achter de software van Bitdefender Password Manager staan enkele van de nieuwste cryptografische algoritmen die de hoogste gegevensbeveiliging garanderen waarop gebruikers kunnen hopen, zoals AES-256-CCM, SH512, BCRYPT, HTTPS- en WSS-protocollen voor gegevensoverdracht. Alle betrokken gegevens worden te allen tijde lokaal versleuteld en ontsleuteld. Dit maakt het mogelijk dat alleen de accounthouder toegang heeft tot de binnen de account opgeslagen informatie, alsmede tot het hoofdwachtwoord dat wordt gebruikt om toegang te krijgen tot en vervolgens gebruik te maken van de gegevens in kwestie.

1.2. 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 Password Manager alleen gebruiken op apparaten met de volgende besturingssystemen:

- **Voor pc-gebruikers:**
  - Windows 7 met Service Pack 1
  - Windows 8
  - 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 Password Manager 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 Password Manager niet kan worden geïnstalleerd of dat het product niet goed functioneert.

2.2. Installatie

In dit hoofdstuk wordt uitgelegd hoe u Bitdefender Password Manager 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**.

1. Ga naar https://central.bitdefender.com/ en log in op uw account.
   Als u nog geen account hebt, klik dan op **CREËER ACCOUNT**, typ uw volledige naam, een e-mailadres en een wachtwoord.
2. Selecteer **Mijn apparaten** in de linkerzijbalk van het scherm.
3. Ga in het onderdeel **Mijn apparaten** verder door te klikken op **+ Apparaat toevoegen**.
4. Door deze actie verschijnt een nieuw venster. Kies **Password Manager** in het selectiescherm.
5. Kies **Dit apparaat**.
   Als u de installatie wilt uitvoeren op een ander apparaat, selecteer dan Andere apparaten. U kunt dan een downloadkoppeling naar het betreffende apparaat e-mailen of de URL voor de installatie kopiëren.
6. Kies vervolgens op welke browser u de Password Manager-extensie wilt installeren.
7. Elke overeenkomstige knop zal u doorverwijzen naar de Extensions Store van de browser. Vanaf daar volgt u gewoon de instructies op het scherm zoals hieronder weergegeven:

   Microsoft Edge

   - Klik op de knop **Kopen**
   - Klik op **Extensie toevoegen** in de prompt die op het scherm verschijnt

   Google Chrome

   - Klik op de knop **Toevoegen aan Chrome**
   - Klik in het bevestigingsvak op **Extensie toevoegen**

   Mozilla Firefox

   - Klik op de knop **Toevoegen aan Firefox**
   - Klik in de rechterbovenhoek van het scherm op de knop **Installeren**

   Safari

   - Klik op de knop **Kopen**, klik dan op **Installeren**
   - Open Safari en selecteer **Voorkeuren** in de bovenste menubalk

- Klik in het venster Voorkeuren op het tabblad **Extensies**.
- Schakel het selectievakje naast Password Manager in om het in te schakelen.

Nadat u deze stappen hebt gevolgd, stelt u een sterk hoofdwachtwoord in en drukt u op de knop **Hoofdwachtwoord opslaan** nadat u de **Voorwaarden** hebt gelezen en ermee akkoord bent gegaan.

Belangrijk

Merk op dat u dit hoofdwachtwoord nodig hebt om alle wachtwoorden, creditcardgegevens en notities die zijn opgeslagen in Bitdefender Password Manager te ontgrendelen. Dit is in wezen de sleutel waarmee de eigenaar dit product kan gebruiken.

Waarschuwing

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

- U kunt op **Sluiten** drukken als u klaar bent.

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.

GET IT ON Google Play

U kunt de Bitdefender Password Manager-app ook installeren via uw **Bitdefender Central**-account:

1. Log op uw mobiel Android-apparaat in op uw Bitdefender Central-account via https://login.bitdefender.com/central/login.
2. Selecteer **Mijn apparaten** in de linkerzijbalk van het scherm.
3. In de **Mijn apparaten** sectie, ga verder door op te klikken **+ Apparaat toevoegen**.

4. Deze actie zorgt ervoor dat er een nieuw venster verschijnt. Kiezen **wachtwoordbeheerder** in het keuzescherm.
5. Kiezen **Dit apparaat**.
   Als u de installatie wilt uitvoeren op een ander apparaat, selecteer dan **Andere apparaten**. U kunt dan een downloadkoppeling naar het betreffende apparaat e-mailen of de URL voor de installatie kopiëren.
6. U wordt doorgestuurd naar **Google Play**. Tik op **Installeren** om Bitdefender Password Manager op Android te downloaden.
7. Zodra het downloaden is voltooid, opent u de Password Manager-applicatie.
8. Als u niet automatisch bent ingelogd op uw account, meld u dan aan met uw gebruikersnaam en wachtwoord.
   Nadat u deze stappen heeft gevolgd, stelt u een sterk hoofdwachtwoord in en drukt u op de **Sla het hoofdwachtwoord op** knop nadat u het hebt gelezen en ermee akkoord gaat **Voorwaarden**.

   Belangrijk
   Merk op dat u dit hoofdwachtwoord nodig hebt om alle wachtwoorden, creditcardgegevens en notities te ontgrendelen die zijn opgeslagen in Bitdefender Password Manager. Dit is in wezen de sleutel waarmee de eigenaar dit product kan gebruiken.

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

   ❍ U kunt op drukken **Dichtbij** wanneer klaar.
9. Maak een **4-cijferige pincode**, zodat u het hoofdwachtwoord niet opnieuw hoeft in te voeren als u naar een andere app overschakelt en weer terug naar Password Manager. Als die beschikbaar is, kunt u ook gezichtsherkenning of vingerafdrukverificatie inschakelen.
10. Tik op **Automatisch invullen inschakelen** om de Android-instellingen voor automatisch instellen te configureren.

> **Opmerking**
> Als u deze stap overslaat, kunt u Android Autofill-functies op een later tijdstip inschakelen en aanpassen door de instructies te volgen die op Intelligente Autofill (pagina 20) beschikbaar zijn.

11. U ziet een lijst met apps die wachtwoorden automatisch kunnen invullen.
    Selecteer **Password Manager**, dan vraagt het apparaat u om te bevestigen dat u de app vertrouwt.
    Tik op **OK**.

12. Voer de pincode in die u in **stap 9** hebt gekozen om de actie te bevestigen

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.

Download on the App Store

Het installeren van de Bitdefender Password Manager-app kan ook via uw Bitdefender Centraal rekening:

1. Log op uw iPhone of iPad in op uw Bitdefender Central-account via https://login.bitdefender.com/central/login.
2. Selecteer **Mijn apparaten** in de linkerzijbalk van het scherm.
3. In de **Mijn apparaten** sectie, ga verder door op te klikken **+ Apparaat toevoegen**.
4. Deze actie zorgt ervoor dat er een nieuw venster verschijnt. Kiezen **wachtwoordbeheerder** in het keuzescherm.
5. Kiezen **Dit apparaat**.
   Als u op een ander apparaat wilt installeren, selecteert u **Andere apparaten**. U kunt vervolgens een downloadlink naar het betreffende apparaat e-mailen of de URL voor de installatie direct kopiëren.

6. U wordt doorgestuurd naar de **App Store**. Tik op het cloudpictogram met een pijl naar beneden om Bitdefender Password Manager voor iOS te downloaden.
7. Zodra de applicatie is geïnstalleerd, opent u deze en vinkt u het kleine vakje op het scherm aan. Selecteer **Doorgaan** nadat u de **Abonnementsovereenkomst** hebt gelezen en ermee akkoord gaat.
8. Als u niet automatisch bent aangemeld bij uw account, meldt u zich aan met uw gebruikersnaam en wachtwoord.
   Nadat u deze stappen heeft gevolgd, stelt u een sterk hoofdwachtwoord in en drukt u op de **Sla het hoofdwachtwoord op** knop nadat u het hebt gelezen en ermee akkoord gaat **Voorwaarden**.

   Belangrijk
   Merk op dat u dit hoofdwachtwoord nodig hebt om alle wachtwoorden, creditcardgegevens en notities te ontgrendelen die zijn opgeslagen in Bitdefender Password Manager. Dit is in wezen de sleutel waarmee de eigenaar dit product kan gebruiken.

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

   ❍ U kunt op drukken **Dichtbij** wanneer klaar.
9. Maak een **4-cijferige pincode**, dus als u overschakelt naar een andere app en vervolgens terugkeert naar Password Manager, hoeft u het eerder ingestelde hoofdwachtwoord niet opnieuw in te voeren. Indien beschikbaar kunt u ook gezichtsherkenning of vingerafdrukverificatie inschakelen.

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

3. GEDEELD ABONNEMENT

Met het Bitdefender Password Manager Shared Plan kunnen meerdere gebruikers toegang krijgen tot hetzelfde abonnement en het gebruiken. Het biedt een gecentraliseerde aanpak voor softwaretoegang, beheer en ondersteuning en biedt een kosteneffectieve oplossing voor het delen van de wachtwoordbeheerservices onder meerdere gebruikers.

- De persoon die verantwoordelijk is voor het gedeelde abonnement, ook wel de Plan Manager genoemd, kan de service onder de leden delen.
- Elk lid krijgt zijn eigen unieke Bitdefender Central-account gekoppeld aan zijn e-mailadres en toegang tot de service Password Manager.

3.1. Bitdefender Wachtwoordbeheer delen met meerdere gebruikers

Leden uitnodigen

Om een of meerdere gebruikers aan het gedeelde abonnement toe te voegen, moet de abonnementsbeheerder deze stappen volgen:

1. Meld u aan bij uw Bitdefender Central-account op https://central.bitdefender.com/.
2. Ga naar het menu **Mijn abonnementen** aan de linkerkant van de pagina.
3. Kies **Lid uitnodigen** in het paneel **Bitdefender Password Manager Shared Plan**.
4. Voer het e-mailadres in van elke persoon met wie u uw abonnement wilt delen en klik vervolgens op**Versturen**. Er kunnen maximaal 3 leden tegelijk worden toegevoegd.
5. De installatie-instructies worden meteen naar de nieuwe leden gemaild. Klik op **Sluiten** om het bevestigingsvenster te sluiten.

> **Opmerking**
> Leden hebben 24 uur de tijd om uw uitnodiging te accepteren zodra deze naar hen is verzonden.
>
> - Uitgenodigde leden verschijnen met de status 'Uitgenodigd'.
> - Je zult ze zien als “Actieve” leden nadat ze de uitnodiging hebben geaccepteerd. U wordt ook per e-mail op de hoogte gesteld van elke geaccepteerde uitnodiging.

Leden verwijderen

Bitdefender Password Manager Shared Plan-toegang gaat verloren voor leden die worden verwijderd. Wanneer de planbeheerder besluit een lid van het abonnement te verwijderen, ontvangt het lid een kennisgeving per e-mail. Gedurende de volgende 30 dagen wordt het ex-lid overgeschakeld op een 30-daagse proefversie van Bitdefender Password Manager met volledige mogelijkheden. Daarna wordt de service uitgeschakeld.

De abonnementsbeheerder kan op de volgende manier gebruikers uit het gedeelde abonnement verwijderen:

1. Meld u aan bij uw Bitdefender Central-account op https://central.bitdefender.com/.
2. Ga naar het menu **Mijn abonnementen** aan de linkerkant van de pagina.
3. Klik in het paneel **Bitdefender Password Manager Shared Plan** op Beheren en kies vervolgens **Leden bewerken** in het menu.
4. Klik op de knop **Verwijderen** om een lid uit het gedeelde plan te verwijderen.
5. Kies **Ja, lid verwijderen** en klik vervolgens op de knop **Bewerken voltooien** om de wijzigingen van kracht te laten worden.

> **Opmerking**
> Wanneer een lid wordt verwijderd uit het gedeelde plan, wordt zijn status gewijzigd in **In afwachting van verwijdering** totdat hij volledig is verwijderd.

Uitnodiging accepteren

U ontvangt een e-mail wanneer iemand u uitnodigt om lid te worden van het Bitdefender Password Manager Shared Plan. U heeft 24 uur de tijd om een uitnodiging te accepteren zodra deze naar u is verzonden.

Om de uitnodiging te accepteren en toegang te krijgen tot de functies van wachtwoordbeheer, moet de gebruiker deze stappen volgen:

1. Open de e-mail die u hebt ontvangen met de titel **[Begin uw Bitdefender-abonnement als lid te gebruiken]** en klik op de knop **ACTIVEREN IN CENTRAL**.
2. De Bitdefender Central-pagina wordt dan geopend in uw browser.
   - Als u al een Bitdefender-gebruikersaccount hebt gekoppeld aan het e-mailadres waar de uitnodiging naartoe werd gestuurd, **meld u dan aan** om uw gedeelde abonnement te claimen.
   - Als u geen Bitdefender-gebruikersaccount hebt, klik dan op **Maak er een** en meld u aan met hetzelfde e-mailadres als waar de uitnodiging naartoe is gestuurd om uw gedeelde abonnement te claimen.
     - Voer uw volledige naam in
     - Voer uw e-mailadres in
     - Voer uw wachtwoord in
     - Klik op de knop Account aanmaken en u wordt aangemeld.
3. Klik na het aanmelden op **Aan de slag** op het welkomstscherm dat u informeert dat uw Bitdefender Password Manager-abonnement nu actief is.
4. Volg de stappen op het scherm die ook worden beschreven in Installatie (pagina 6).

> **Opmerking**
>
> De e-mail van de abonnementsbeheerder wordt weergegeven in uw Bitdefender Central-account bovenaan het menu Wachtwoordbeheerder en op de abonnementskaart, onder Mijn abonnementen.
>
> Als u hulp nodig heeft bij het gedeelde plan, neem dan contact met hen op.

4. 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.

4.1. Compatibiliteit

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

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

- **Panda Dome Passwords**
- **PassWatch**
- **Saferpass**
- **SFR Cybersécurité**
- **SIT**
- **F-Secure**
- **Telnor**

> **Opmerking**
> Als de naam van de browser of het wachtwoordbeheerprogramma van waaruit u gegevensbestanden probeert over te zetten niet wordt vermeld in bovenstaande lijst, kunt u onze online gids volgen over hoe gebruikers een CSV-bestand van niet-ondersteunde wachtwoordbeheerders kunnen bewerken, zodat u uw informatie kunt importeren in **Bitdefender Password Manager**: https://www.bitdefender.nl/consumer/support/answer/14622/

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**.

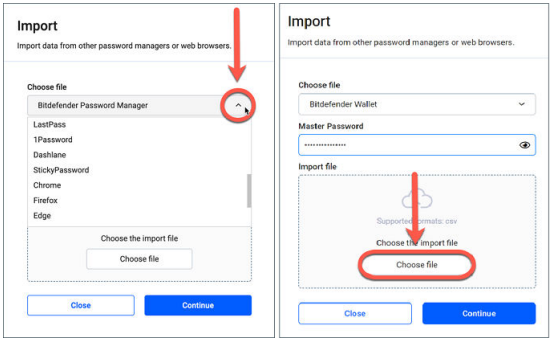
4.2. Importeren in Password Manager

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. Klik op het Password Manager-pictogram in uw webbrowser (op Windows of macOS) of start de Password Manager-applicatie (op Android of iOS). Voer uw hoofdwachtwoord **in als daarom wordt gevraagd**.
2. Open het menu Password Manager om de zijbalk aan de linkerkant uit te vouwen en klik op het menu-item **Instellingen**.
3. Scroll naar beneden naar het onderdeel **Gegevens** en klik op de optie **Gegevens importeren**.
4. Selecteer in het drop-down menu de wachtwoordbeheer-app of browser waaruit u uw accounts wilt importeren, voer uw **Hoofdwachtwoord** in het betreffende veld in en klik vervolgens op **Bestand kiezen**.



5. Blader door uw mappen om de locatie te vinden waar u het bestand met uw gebruikersnamen en wachtwoorden hebt opgeslagen, geëxporteerd vanuit uw andere wachtwoordbeheerder of webbrowser, en druk vervolgens op de knop **Doorgaan**.

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

4.3. 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. Klik op het Password Manager-pictogram in uw webbrowser (op Windows of macOS) of start de Password Manager-toepassing (op Android of iOS). Voer desgevraagd uw Master wachtwoord.
2. Open het menu Password Manager om de linkerzijbalk uit te vouwen en klik op het menu-item **Instellingen**.
3. Scroll naar beneden naar het onderdeel **Gegevens** en klik op de optie **Gegevens exporteren**.
4. Op dit punt zou u de volgende twee opties te zien moeten krijgen:
   - **CSV**
   - **Wachtwoord-beveiligde bestanden**

   Selecteer de optie van uw voorkeur, voer uw hoofdwachtwoord in en klik op de knop **Gegevens exporteren**.

   > **Opmerking**
   > Als u de optie Wachtwoord-beveiligd bestand kiest, wordt u gevraagd de lijst met accounts met een wachtwoord te versleutelen, zodat alleen u er toegang toe hebt, indien nodig.

5. Uw webbrowser/app zal onmiddellijk een bestand met de naam Bitdefender Password Manager_exported_data_current-date op uw systeem opslaan in de standaarddownloadmap. Het bevat al uw gegevens die in Bitdefender Password Manager zijn opgeslagen.

Nadat u uw gegevens hebt geëxporteerd, kunt u deze uploaden naar de wachtwoordbeheerder van uw keuze.

5. 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.

5.1. Wachtwoordbehandeling

5.1.1. Wachtwoordgenerator

De gouden regel met betrekking tot online beveiliging is om altijd unieke, willekeurige wachtwoordzinnen te gebruiken voor elke dienst waarvoor een account moet worden aangemaakt. Hergebruik van wachtwoorden op meerdere platforms is de belangrijkste reden voor identiteitsdiefstal en verliezen in verband met vijandige overname van accounts.

Deze functie helpt gebruikers met het genereren van veilige, complexe en unieke wachtwoorden voor elke nieuwe account die ze ergens online aanmaken. Hierdoor hoeven gebruikers zelf geen sterke wachtwoorden meer te verzinnen of op te letten dat ze hetzelfde wachtwoord niet hergebruiken voor meerdere accounts.

De **Wachtwoordgenerator** is toegankelijk via het tabblad bovenaan de interface van Password Manager.

De generator kan worden ingesteld om wachtwoorden **tussen 4 en 32 tekens** te maken.

U kunt ook de soorten tekens specificeren die al dan niet aanwezig moeten zijn in het willekeurig gegenereerde wachtwoord door de overeenkomstige vakjes aan of uit te vinken. **(Kleine letters, Hoofdletters, Cijfers, Speciale tekens)**

Door op de knop rechts van het weergegeven wachtwoord te drukken, zal de generator het voorgestelde wachtwoord wijzigen.

Om het getoonde wachtwoord te gebruiken, drukt u op **Wachtwoord gebruiken**, een actie die de tekenreeks zal opslaan op uw klembord.

> **Opmerking**
> Uw eerder gegenereerde wachtwoorden worden tijdelijk opgeslagen in de wachtwoordgeschiedenis, die toegankelijk is via de knop **Wachtwoordgeschiedenis**.

5.1.2. Vastleggen van wachtwoorden

Met deze functie in Password Manager wordt u gevraagd om al uw nieuwe wachtwoorden op te slaan onmiddellijk na het aanmaken ervan. Password Manager vraagt gebruikers om hun nieuw aangemaakte wachtwoorden op te slaan, zodat ze meteen kunnen worden toegevoegd aan de ultraveilige omgeving die Bitdefender biedt.

5.1.3. Intelligente Autofill

Bitdefender Password Manager kan zo worden ingesteld dat uw aanmeldingsgegevens en vooral wachtwoorden automatisch worden ingevuld. Bedrijfseigen algoritmen kunnen aanmeldingsgegevens op eerder bezochte websites detecteren en vooraf invullen, waardoor de gebruikers elke keer dat ze zich bij een dienst aanmelden, tijd besparen.

1. Klik in Windows of macOS op het **Password Manager** pictogram in uw webbrowser.

   Start op Android of iOS de **Password Manager**-applicatie.
   Voer uw **Hoofdwachtwoord** in als daarom wordt gevraagd.

2. Open het menu Password Manager om de zijbalk aan de linkerkant uit te vouwen en klik op het menu-item **Instellingen**.

3. Klik op **Apparaatinstellingen**.

4. Hier ziet u een knop met **Automatisch invullen uitschakelen** of **Automatisch invullen inschakelen**. Deze instelling bepaalt de werking van de intelligente automatisch invulfunctie.

5.1.4. Beveiligingsrapport

Het Beveiligingsrapport is een hulpmiddel dat rapporten genereert op basis van een aantal kenmerken om uw digitale veiligheid te verbeteren. Het laat u weten of een wachtwoord uw onmiddellijke aandacht vereist door het bepalen van het beveiligingsniveau. Het detecteert dubbele wachtwoorden en vraagt u deze te veranderen, zodat u niet het risico loopt hetzelfde wachtwoord voor meerdere accounts te gebruiken.

Het rapport is gericht op het verstrekken van informatie over uw algemene wachtwoordhygiëne: dit betreft dubbele wachtwoorden, zwakke of anderszins gelekte wachtwoorden of e-mailadressen.

Dit wordt gedaan door de lijst met versleutelde hashes van Troy's webpagina lokaal op uw apparaat te vergelijken, om te controleren of deze de overeenkomstige hashes van uw wachtwoorden bevat. Als er een overeenkomst wordt gevonden, wordt u gewaarschuwd om u aan te moedigen uw wachtwoorden en andere aanmeldingsgegevens te wijzigen.

Om het **Beveiligingsrapport** te openen, opent u de Password Manager-interface en selecteert u de bijbehorende knop in de bovenste balk.

5.1.5. Synchronisatie met andere platformen

Door uw wachtwoorden eenmaal op te slaan in Bitdefender Password Manager kunt u ze bewaren en veilig openen op al uw Windows-, Mac-, Android- of iOS-apparaten vanuit Chrome, Safari, Firefox en Edge of in mobiele apps.

> **Opmerking**
> Bitdefender is ook uitgerust met een **offline modus** voor toegang tot uw wachtwoorden, mocht u toevallig geen toegang hebben tot het internet. Hierdoor zijn uw wachtwoorden altijd en overal toegankelijk.

5.1.6. Een invoer verwijderen

Om opgeslagen wachtwoorden te verwijderen, drukt u eerst op het bewerkingspictogram naast de invoer die u wilt verwijderen, in het tabblad **Accounts**. Scroll naar beneden en kies **Verwijderen**. Wanneer u wordt gevraagd of u zeker weet dat u de account wilt verwijderen, kiest u **Verwijderen**.

5.2. Accountbehandeling

5.2.1. Authenticatie

De authenticatie in Bitdefender Password Manager gebeurt via de **pincode** die is ingesteld tijdens het installatieproces van het product. (Merk op dat de functie {3}Auto-Lock{4} de wachtwoordmanager vergrendelt of uitlogt na een periode van inactiviteit op browserniveau of het sluiten van de mobiele app).

Daarnaast kan het ook gebeuren door het gebruik van biometrie, indien beschikbaar, zoals **Vingerafdruk** of **Gezichtsontgrendeling**.

Om biometrische authenticatie **in of uit te schakelen**:

1. Klik in Windows of macOS op de **Password Manager** pictogram in uw webbrowser.

   Start op Android of iOS het **Password Manager** sollicitatie.
   Voer desgevraagd uw Master wachtwoord.

2. Open het Wachtwoordbeheer-menu om de zijbalk aan de linkerkant uit te vouwen en klik op de **Instellingen** menu onderdeel.

3. Klik op **Apparaat instellingen**.

4. Hier ziet u een knop met **Biometrie uitschakelen** of **Biometrie inschakelen**. Deze instelling bepaalt de werking van de biometrische authenticatiefunctie.

5.2.2. Hoofdwachtwoord opnieuw instellen

> **Belangrijk**
> De functie **Hoofdwachtwoord wijzigen** is niet beschikbaar op mobiele apparaten. De enige manier waarop u uw hoofdwachtwoord kunt wijzigen of herstellen is via de Bitdefender Password Manager browserextensie op een Windows-pc of een macOS-apparaat.

Zo wijzigt u uit voorzorg uw **Hoofdwachtwoord** en maakt u een nieuw aan in Bitdefender Password Manager:

1. Zodra u de browserextensie hebt geïnstalleerd, klikt u op het **Password Manager** pictogram in de werkbalk van uw webbrowser.

2. Voer uw huidige hoofdwachtwoord in om de kluis te ontgrendelen.

> **Belangrijk**
> Als u het huidige hoofdwachtwoord vergeten bent, klikt u op de optie **Ik ben mijn wachtwoord vergeten** op hetzelfde scherm. Voer de **24-cijferige herstelsleutel** in die werd verstrekt tijdens de eerste installatie van Bitdefender Password Manager, en typ vervolgens een nieuw hoofdwachtwoord. **Als u** zowel het **hoofdwachtwoord** als de **herstelsleutel** vergeet of kwijt raakt, kunt u als laatste redmiddel **contact opnemen met een vertegenwoordiger van Bitdefender om u te helpen uw account opnieuw in te stellen**. Als uw account opnieuw wordt ingesteld, worden **al uw gegevens en wachtwoorden** die in Bitdefender Password Manager zijn opgeslagen, gewist.

3. Open het Wachtwoordbeheer-menu om de zijbalk aan de linkerkant uit te vouwen en klik op de **Instellingen** menu onderdeel.
4. Klik op de **Mijn account** knop in het onderdeel **Account**.
5. Er verschijnt een venster met informatie over uw abonnement op Password Manager.
   Klik op de knop **Hoofdwachtwoord wijzigen**.
6. U wordt doorgestuurd naar een nieuw venster waar u een nieuw hoofdwachtwoord kunt kiezen. Voer uw huidige hoofdwachtwoord in en typ vervolgens een nieuw hoofdwachtwoord. Het nieuwe hoofdwachtwoord moet minstens 8 tekens bevatten, minstens één kleine letter, één hoofdletter en één cijfer.
7. Druk op de knop **Wijzigen** als u klaar bent.
8. Wacht even totdat Bitdefender het oude hoofdwachtwoord opnieuw instelt.
   Sluit uw webbrowser niet af!
9. Vervolgens krijgt u een nieuwe **24-cijferige herstelsleutel**. Noteer de herstelsleutel op een veilige plaats en **raak hem niet kwijt**. Deze sleutel is de enige manier om toegang te krijgen tot uw wachtwoorden die zijn opgeslagen in Password Manager in het geval u het hoofdwachtwoord vergeet.
   Druk op **Sluiten** als u klaar bent.
10. U wordt uitgelogd bij Bitdefender Password Manager.
    Om de kluis te ontgrendelen, gebruikt u het nieuwe hoofdwachtwoord dat u zojuist hebt ingesteld.

5.3. Andere functionaliteiten

5.3.1. Identiteitbeheer

Met deze functie kunnen gebruikers meerdere identiteiten opslaan en kan Password Manager op een snelle, gemakkelijke en veilige manier automatisch gegevens in webformulieren invullen voordat ze een aankoop doen.

Zoals alles in Password Manager zijn alle gevoelige gegevens in deze opgeslagen identiteiten versleuteld en alleen beschikbaar voor het apparaat van de gebruiker.

Om een identiteit toe te voegen aan Password Manager:

1. Klik in Windows of macOS op de **Password Manager** pictogram in uw webbrowser.

   Start op Android of iOS het **Password Manager** sollicitatie.
   Voer desgevraagd uw Master wachtwoord.

2. Open het menu Password Manager om de zijbalk aan de linkerkant uit te vouwen en klik op het menu-item **Identiteiten**.
3. Druk op de knop **Identiteit toevoegen** onderaan.
4. Vul de gegevens in die u wilt bewaren en druk vervolgens op **Opslaan**.

5.3.2. Creditcardbeheer

Met deze functie kunt u creditcardgegevens opslaan en invullen om gemakkelijker, sneller en veiliger te winkelen.

Om een creditcard toe te voegen aan Password Manager:

1. Klik in Windows of macOS op de **Password Manager** pictogram in uw webbrowser.

   Start op Android of iOS het **Password Manager** sollicitatie.
   Voer desgevraagd uw Master wachtwoord.

2. Open het menu Password Manager om de zijbalk aan de linkerkant uit te vouwen en klik op het menu-item **Creditcards**.
3. Druk op de **Identiteit toevoegen** knop onderaan.
4. Vul de gegevens in die u wilt opslaan en druk op **Redden**.

5.3.3. Secure Me (Beveilig mij)

Met de Secure Me-functie kunt u zich op afstand afmelden of de browsegeschiedenis van uw computer, tablet of mobiele apparaat wissen. Als u een apparaat met andere mensen deelt, raden wij u ten zeerste aan deze functie in te schakelen.

Om deze functie te lokaliseren en in te schakelen:

1. Klik in Windows of macOS op de **Password Manager** pictogram in uw webbrowser.

   Start op Android of iOS het **Password Manager** sollicitatie.

Voer desgevraagd uw Master wachtwoord.

2. Open het menu Password Manager om de zijbalk aan de linkerkant uit te vouwen en klik op het menu-item **Secure Me**.
3. Druk op de knop **Alle sessies beveiligen**.
   Als u alleen een bepaald apparaat wilt beveiligen, zoekt u het in de lijst met apparaten waarop Password Manager is geïnstalleerd of ingeschakeld in een specifieke browser.

5.3.4. Notities

Secure Notes werken net als een geheim notitieboek waarin u gevoelige gegevens kunt opslaan, sorteren en kleurcodering kunt gebruiken om ze beter te visualiseren. Zo houdt u niet alleen informatie netjes, maar ook veilig en beschermd.

Om deze functie te lokaliseren en in te schakelen:

1. Klik in Windows of macOS op de **Password Manager** pictogram in uw webbrowser.
   Start op Android of iOS het **Password Manager** sollicitatie.
   Voer desgevraagd uw Master wachtwoord.
2. Open het menu Password Manager om de zijbalk aan de linkerkant uit te vouwen en klik op het menu-item **Notities**.
3. Druk op de knop **Note toevoegen**.
   Zodra u de informatie die u wilt bewaren hebt opgeschreven, drukt u op **Opslaan**.

6. 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

Hoe kan ik de pop-up Password Manager die wordt weergegeven in mijn beveiligingsoplossing van Bitdefender stoppen?

De melding Password Manager die in augustus 2022 werd weergegeven door Bitdefender Total Security, Internet Security en Antivirus Plus, kan worden gesloten door op de knop "x" te klikken. Het venster "Beheer uw wachtwoorden met Bitdefender Password Manager" zal willekeurig nog twee keer verschijnen voordat het voorgoed verdwijnt. Dit type in productcommunicatie kan worden gestopt door de schakelaar **Aanbeveling notificaties** in Bitdefender-instellingen uit te schakelen.

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 @).

Hoe kan ik voorkomen dat Bitdefender elke keer als ik de browser open, om mijn hoofdwachtwoord vraagt?

Als u uw apparaat vergrendelt zonder de browser te sluiten, wordt Password Manager niet vergrendeld en hebt u toegang tot uw gegevens wanneer u terugkeert. Als veiligheidsmaatregel moet u zich elke keer dat u de browser opent aanmelden met uw Bitdefender Central-account en vervolgens uw hoofdwachtwoord invoeren.

- Om de pop-up voor het aanmelden bij Bitdefender Central te stoppen, gaat u naar Instellingen en vinkt u de optie "Tabblad Aanmelden bij opstarten uitschakelen" aan.
- Om de hoofdwachtwoordprompt te voorkomen, vinkt u het vakje "Onthoud mij" aan in het scherm Uw kluis ontgrendelen.

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.

Als u zowel het hoofdwachtwoord als de herstelsleutel bent vergeten of kwijtgeraakt, kunt u als laatste redmiddel contact opnemen met een Bitdefender-vertegenwoordiger om uw account opnieuw in te stellen.

> **Belangrijk**
> Als u uw account opnieuw instelt, worden al uw gegevens en wachtwoorden die zijn opgeslagen in Bitdefender Password Manager gewist.

Kunnen meerdere gebruikers een abonnement op Bitdefender Password Manager delen?

Op dit moment is de mogelijkheid om meerdere gebruikers op hetzelfde Bitdefender Password Manager-abonnement te hebben niet beschikbaar, maar we zijn van plan om deze functie in de toekomst in te schakelen.

Wat is de Offline modus en hoe werkt deze?

De Offline modus wordt automatisch geactiveerd wanneer de internetverbinding wegvalt tijdens het gebruik van Bitdefender Password Manager. Als u al bent aangemeld en uw hoofdwachtwoord hebt ingevoerd, hebt u in de offline modus toegang tot uw wachtwoorden wanneer er geen internetverbinding meer 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.

7. HULP VRAGEN

7.1. 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.

7.2. 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.

7.2.1. 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/.

7.2.2. 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/

7.2.3. 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/.

7.3. 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/

7.3.1. 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.